Computing canonical heights on Jacobians

Von der Universität Bayreuth
zur Erlangung des Grades eines
Doktors der Naturwissenschaften (Dr. rer. nat.)
genehmigte Abhandlung

von

Jan Steffen Müller

aus Gießen

1. Gutachter: Prof. Dr. Michael Stoll
2. Gutachter: Prof. Dr. Victor Flynn

Tag der Einreichung: 6.10.2010
Tag des Kolloquiums: 16.12.2010

Abstract

The canonical height is an indispensable tool for the study of the arithmetic of abelian varieties. In this dissertation we investigate methods for the explicit computation of canonical heights on Jacobians of smooth projective curves. Building on an existing algorithm due to Flynn and Smart with modifications by Stoll we generalize efficient methods for the computation of canonical heights on elliptic curves to the case of Jacobian surfaces. The main tools are the explicit theory of the Kummer surface associated to a Jacobian surface which we develop in full generality, building on earlier work due to Flynn, and a careful study of the local Néron models of the Jacobian.

As a first step for a further generalization to Jacobian threefolds of hyperelliptic curves, we completely describe the associated Kummer threefold and conjecture formulas for explicit arithmetic on it, based on experimental data. Assuming the validity of this conjecture, many of the results for Jacobian surfaces can be generalized.

Finally, we use a theorem due to Faltings, Gross and Hriljac which expresses the canonical height on the Jacobian in terms of arithmetic intersection theory on a regular model of the curve to develop an algorithm for the computation of the canonical height which is applicable in principle to any Jacobian. However, it uses several subroutines and some of these are currently only implemented in the hyperelliptic case, although the theory is available in general.

Among the possible applications of the computation of canonical heights are the determination of generators for the Mordell-Weil group of the Jacobian and the computation of its regulator, appearing for instance in the famous Birch and Swinnerton-Dyer conjecture. We illustrate our algorithm with two examples: The regulator of a finite index subgroup of the Mordell-Weil group of the Jacobian of a hyperelliptic curve of genus 3 and the non-archimedean part of the regulator computation for the Jacobian of a non-hyperelliptic curve of genus 4, where the remaining computations can be done immediately once the above-mentioned implementations are available.

Acknowledgements

First I would like to thank my advisor Michael Stoll for suggesting this research project to me, for many useful ideas and discussions and for answering a lot of questions, occasionally several times.

I would like to thank my parents for always supporting me and believing in me, especially during those times when I found it hard to do so myself.

I wish to acknowledge financial support from Jacobs University Bremen (2006–2007) and from Deutsche Forschungsgemeinschaft (DFG-Grant STO 299/5-1, 2007–2010).

I would like to thank my colleagues Brendan Creutz and Tzanko Matev for interesting mathematical and non-mathematical discussions in Bremen, Bayreuth and in other places; special thanks are due to Tzanko for providing me with a proof of Proposition 4.1. I would also like to thank Elvira Rettner and Axel Kohnert for helping me with many practical problems in Bayreuth.

I was very fortunate to have the opportunity to visit several mathematical institutions during my work on this thesis; I would like to thank the following mathematicians for either inviting me to their institutions, helping me with my research and/or supporting my visits financially: Samir Siksek and David Holmes at the University of Warwick, Victor Flynn at the University of Oxford, Ulf Kühn and Vincenz Busch at the Universität Hamburg, Kiran Kedlaya and Jen Balakrishnan at MIT and Sylvain Duquesne at the Université Rennes I.

Thanks are also due to Steve Donnelly of the Magma group at the University of Sydney for writing the RegularModel package in `Magma` which large parts of the algorithm presented in Chapter 5 rely on, taking into account my (rather long) wish list.

Furthermore, I have had useful conversations, in person or by email, with a large number of mathematicians. Among those I would like to thank whose names have not yet appeared in these acknowledgments are Karim Belabas, Dominique Bernardi, Antoine Chambert-Loir, Pierre Chrétien, Brian Conrad, Christian Curilla, Bernard Deconinck, Robin De Jong, Stephan Elsenhans, Pierrick Gaudry, Florian Hess, Marc Hindry, Qing Liu, Jean-François Mestre, Michael Mourao, Fabien Pazuki, Cédric Pepin, Anna Posingies, Christophe Ritzenthaler, Mohammad Sadek, Joe Silverman, Damiano Testa, Yukihiro Uchida and Kentaro Yoshitomi.

für Tonia

Contents

Introduction **xiii**
Organization xvii

1 Motivation and background **1**
1.1 Places and absolute values 2
1.2 Heights 3
1.3 Néron functions 5
1.4 Néron models 8
1.5 Curves and Jacobians 11
1.6 Theta functions 19
1.7 Applications 21

2 Elliptic curves **25**
2.1 Heights on elliptic curves 26
2.2 Local heights 26
2.3 Non-archimedean places 30
2.4 Archimedean places 35

3 Jacobian surfaces **39**
3.1 Jacobian surfaces and Kummer surfaces 40
3.2 Canonical heights on Jacobian surfaces 43
3.2.1 Global construction 43
3.2.2 The algorithm of Flynn and Smart 46
3.2.3 Stoll's refinements 47
3.2.4 The "kernel" of ε_v 49
3.3 Kummer surfaces for general models 52
3.3.1 Embedding the Kummer surface in arbitrary characteristic 53
3.3.2 Duplication 55
3.3.3 Biquadratic forms 58
3.3.4 Translation by a point of order 2 59
3.4 Local heights for general models 62
3.4.1 Definitions and first properties 62

3.4.2 The "kernel" of ε_v revisited . . . 68
3.4.3 Relation to Néron models . . . 70
3.4.4 Simplifying the model . . . 73
3.5 Igusa invariants . . . 79
3.6 Formulas for local error functions . . . 84
3.6.1 Case (1) . . . 85
3.6.2 Case (2) . . . 89
3.6.3 Case (3) . . . 91
3.6.4 Case (4) . . . 94
3.6.5 Case (5) . . . 101
3.7 Archimedean places . . . 105
3.7.1 Approximating μ_v using a truncated series . . . 105
3.7.2 Theta functions . . . 106
3.7.3 Richelot isogenies . . . 108

4 Jacobian threefolds 111
4.1 Embedding the Kummer variety . . . 112
4.2 Defining equations for the Kummer variety . . . 115
4.3 Remnants of the group law . . . 118
4.4 Canonical local heights on Jacobians . . . 127
4.4.1 Non-archimedean places . . . 130
4.4.2 Archimedean places . . . 130

5 Arithmetic intersection theory 133
5.1 Local Néron symbols . . . 134
5.2 Global Néron symbols and canonical heights . . . 138
5.2.1 Representing and reducing divisors . . . 141
5.2.2 Mumford representation of divisors on hyperelliptic curves . . . 143
5.3 Computing the global Néron symbol . . . 144
5.3.1 Finding suitable divisors of degree zero . . . 145
5.3.2 Determining relevant non-archimedean places . . . 147
5.3.3 Regular models . . . 148
5.3.4 Computing non-archimedean intersection multiplicities 149
5.3.5 Computing the correction term . . . 158
5.3.6 Computing archimedean intersection multiplicities . . 159

6 Examples and timings 163
6.1 Jacobian surfaces . . . 164
6.1.1 Computing heights . . . 164
6.1.2 Improving the bound on the height constant . . . 166
6.2 Intersection theory . . . 169
6.2.1 Hyperelliptic curves . . . 169
6.2.2 Non-hyperelliptic curves . . . 172

A Proofs of some results from Chapter 3 **179**
A.1 Proof of Lemma 3.16 179
A.2 Proof of Lemma 3.18 181
A.3 Proof of Proposition 3.28 188
A.4 Proof of Lemma 3.46 191
A.5 Proof of Lemma 3.47 193
A.6 Proof of Lemma 3.53 194
A.7 Proof of Proposition 3.56 196
A.8 Proof of Theorem 3.62 203
A.9 Proof of Theorem 3.74 217

Bibliography **223**

List of Figures

1.1 Models of $E : y^2 = x^3 + p^6$ over S 17

3.1 The special fiber of reduction type $[I_m - 0 - 0]$ 86
3.2 The special fiber of reduction type $[I_{m_1 - m_2 - 0}]$ 89
3.3 The special fiber of reduction type $[I_{m_1 - m_2 - m_3}]$ 92
3.4 The special fiber of reduction type $[I_0 - I_0^* - 0]$ 95
3.5 The special fiber of reduction type $[I_0 - IV - l]$ 95
3.6 The special fiber of reduction type $[I_{m_1} - IV^* - l]$ 102

Introduction

If A is an abelian variety defined over a number field k and D is a divisor on A with ample and symmetric linear equivalence class, then we can associate a height function $h_D : A(\bar{k}) \longrightarrow \mathbb{R}$ to D which measures the arithmetic complexity of points on A. This construction is only well-defined up to a bounded function, but we can choose a function $\hat{h}_D$ among these height functions with certain nice properties; for instance, $\hat{h}_D$ is a nonnegative quadratic form that vanishes only on torsion points of A. The original construction of these *canonical heights* is due to Néron [78] and Tate.

In this thesis we are concerned with practical methods for the computation of canonical heights on certain abelian varieties, namely on Jacobians of smooth projective curves. This is useful in several situations:

- First, computing canonical heights is required if we want to find generators of the finitely generated Mordell-Weil group $A(k)$ whenever $A(k)$ has positive rank. See for example [94, §7].

- Second, the celebrated Birch and Swinnerton-Dyer conjecture for elliptic curves [5], one of the seven Clay Millenium Prize problems, has been generalized to arbitrary abelian varieties over number fields by Tate [101]. It has two parts and in order to verify the second part in examples, we need to be able to compute the regulator of the Mordell-Weil group, defined in terms of the canonical height.

- The third application that should be mentioned is the determination of all integral points on smooth projective curves defined over $\mathbb{Q}$. See [14] for an algorithm that uses, among other ingredients, generators of the Mordell-Weil group of the Jacobian of the curve and has proved to be quite successful in genus 2.

For the remainder of this introduction suppose for simplicity that $k = \mathbb{Q}$. The explicit computation of the canonical height of a $\mathbb{Q}$-rational point P on an elliptic curve E has been studied for at least three decades, starting with Tate, some of whose results are reprinted in [89, Chapter VI], and can by now be done very quickly, see [23, §7.5]. Other notable contributions came from Tschöpe and Zimmer [102] and Silverman [87]. Here one uses $D = 2(O)$, where $O \in E$ is the identity element. The most successful approach is to decompose the canonical height into canonical local heights, one for each place $v \in M_{\mathbb{Q}}$. Put differently, we can write

$$\hat{h}(P) = h(P) - \sum_{v \in M_{\mathbb{Q}}} \mu_v(P),$$

where, assuming $P \neq O$, the *naive height* $h(P)$ is the height of the x-coordinate $x(P)$ and the local error functions μ_v measure the difference between the canonical and naive height locally.

It turns out (see [87]) that we can normalize the μ_v in such a way that for prime numbers p we can have $\mu_p(P) \neq 0$ only if p has bad reduction. In these cases the canonical height can be computed easily once we know what the Néron model of E at p looks like. This information can be obtained using Tate's algorithm reproduced in [89, §IV.9]. If $v = \infty$, then there are different methods available: We can use a decomposition of $\mu_\infty(P)$ into an infinite series to approximate $\mu_\infty(P)$. This approach is due to Tate with modifications by Silverman [87]. We can also express $\mu_\infty(P)$ in terms of the Weierstrass σ-function (see [89, Chapter VI]) or we can use the behavior of $\mu_\infty(P)$ under isogenies and a trick involving the quadratically converging arithmetic-geometric mean, which is due to Bost and Mestre [12] and turns out to be the fastest algorithm of the three.

The aim of the first part of this thesis is to generalize these methods to Jacobians of dimension at least 2. In the case of a Jacobian surface J we can build on an existing algorithm due to Flynn and Smart [43] with modifications by Stoll [94]. It uses the Kummer surface K associated to J and remnants on K of the group law on J presented in [41] – in particular, the fact that duplication on J is represented by explicitly known quartic polynomials on K – but requires the computation of (possibly large) multiples of points on J or K.

Although all three algorithms for the computation of $\mu_\infty(P)$ available for elliptic curves can be generalized to the present situation, it turns out that currently the generalization of the series approach of Tate, already introduced by Flynn and Smart, is faster than the other two.

Concerning non-archimedean local error functions, we have succeeded in generalizing the relevant algorithms for elliptic curves to the situation of Jacobian surfaces in that the values of the local error functions $\mu_p(P)$ can now be computed using similar formulas. Our algorithm has been implemented in the computer algebra system `Magma` [67].

However, in contrast to the elliptic curve situation we have to allow some extensions whose ramification indices can be controlled easily. This is a compromise between working over the (local) ground field and working over an extension such that the given model of the curve becomes semistable. We allow extensions such that we can always reduce to a list of essentially five different reduction types. This is possible, because we can find simple formulas expressing how a change of model of the curve affects $\mu_p(P)$.

In order to determine formulas for the computation of $\mu_p(P)$ in these cases, it is useful to study the interplay between μ_p and the Néron model of J over $\mathrm{Spec}(\mathbb{Z}_p)$. Unfortunately, this is more complicated than for elliptic curves and new problems appear, but for a class of reduction types which includes the semistable models we can still get a rather strong statement.

Residue characteristic 2 is, as usual, the trickiest case. In order to deal

with it we first have to generalize the explicit theory of the Kummer surface, previously only worked out for simplified models and characteristic not equal to 2, to arbitrary ground fields and more general models. This has other applications as well, for instance in cryptography as in [34]. One can also use the Kummer surface to search for points on the Jacobian similarly to [96].

Another application of our algorithm is an improvement of the bound on the *height constant*, that is the maximal difference between the naive and the canonical height. Such bounds are important for the computation of generators of the Mordell-Weil group. For Jacobian surfaces, methods for the computation of bounds are discussed in [42], [43], [92], [94] and [103].

Having dealt with Jacobian surfaces, the next step is to generalize our methods to Jacobians of hyperelliptic curves of genus 3. The first task is to find the Kummer variety K and how the group law on J is reflected on it. Earlier works in this direction are [100] and [32]. We have succeeded in completely describing K; however, it is a rather complicated object, namely an intersection of a quadric and 34 quartics in $\mathbb{P}^7$. We hope that this can be used, for instance, to search for points on the Jacobian as in [96]. The traces of the group law are more difficult to find. We prove that certain biquadratic forms, fundamental for describing how addition on a Jacobian surface is reflected on its Kummer surface, cannot exist in this situation.

We have attempted to work around this problem and have stated a conjecture, based on experimental data, that it is still possible to describe duplication on J using quartic polynomials on K and we show how to find candidates for these polynomials. If this conjecture holds, then we can generalize many of our previous results – at least in principle, since the algebra involved is much more difficult. In fact, proving our conjecture is also made more difficult by this issue and it appears that we need some new ideas to tackle the problem.

The observation that the previous approach quickly becomes infeasible as we increase the dimension of the Jacobian naturally leads to a search for other methods. Fortunately, there is a completely different way to express the canonical height on a Jacobian J of a curve C, due to Faltings [37], Gross [46] and Hriljac [52], [53], all using earlier results of Néron [78]. This expression is in terms of arithmetic intersection theory on a reagular model of *the curve*; more precisely, we can decompose the canonical height $\hat{h}(P)$ into a sum of *local Néron symbols* $\langle D, E\rangle_v$, one for each place v of k. Here D and E are divisors of degree zero on the curve with disjoint support that both represent P.

Assuming $k = \mathbb{Q}$ again, we can express $\langle D, E\rangle_p$ for prime numbers p using intersection theory on a regular model of C over $\mathrm{Spec}(\mathbb{Z}_p)$. Our task

is to make this practical by developing algorithms for determining suitable divisors D and E, for finding those p that may yield non-trivial local Néron symbols and for intersection multiplicity computations on regular models. Such models can be computed using `Magma`. Our algorithms rely heavily on Gröbner basis computations and have been implemented in `Magma`; they are most successful for hyperelliptic curves. Another quite similar approach has been developed independently by Holmes and is presented in [50].

The archimedean local Néron symbol $\langle D, E\rangle_\infty$ is defined in terms of Green's functions on the Riemann surface associated to the curve. Building on earlier work by Hriljac, we show how the symbol can be expressed using theta functions on the analytic Jacobian. Again, this is due independently to Holmes [50]. In the hyperelliptic case all necessary computations are possible using existing `Magma` functionality. For non-hyperelliptic curves there are algorithms [7], [29], [30] due to Deconinck et al. for these computations, and even implementations that used to work in earlier versions of `Maple` [68]; they are currently being rewritten in `Sage` [91].

Regarding the ground field, we do not restrict to number fields, since almost all of our results continue to hold if we work over a one-dimensional function field k with perfect residue fields. Indeed, the previous algorithm for genus 2 was only guaranteed to work for global fields but we require no such restriction on k.

Organization

For convenience we now provide a brief summary of the chapters of this thesis.

Chapter 1. Motivation and Background

In this chapter we review some of the theory that we will need later on and explain why the search for methods for the computation of canonical heights is an interesting problem. First we briefly discuss the theory of places and absolute values and fix some normalizations in force throughout this thesis. Next we introduce heights and in particular canonical heights on abelian varieties in Section 1.2. In order to compute the latter, at least when we have a Jacobian of small dimension, we shall use a decomposition into (canonical) local heights as in Section 1.3.

In the non-archimedean case it turns out to be fruitful to investigate the relations between canonical local heights and Néron models, which we do in Section 1.4. This is especially true in the case of Jacobians, since then we can express the Néron model in terms of certain models of the

underlying curve. This is the subject of Section 1.5, where we also introduce several other concepts needed in later chapters. In Section 1.6 we treat archimedean canonical local heights before presenting a short selection of possible applications in the final Section 1.7.

Chapter 2. Elliptic Curves

This chapter presents no original research; we are content to discuss the known results and algorithms briefly, sometimes from a different point of view than what can be found in the literature. We do so because the techniques used in this chapter and our treatment of them are a source of inspiration for the case of higher dimensional Jacobians, especially for Jacobian surfaces that are considered in the following chapter.

In Section 2.1 we introduce heights and canonical heights on elliptic curves using our constructions from the previous chapter. Then we decompose the canonical heights into canonical local heights in Section 2.2, also stating some results and constructions that will we shall imitate in higher-dimensional situations. The computation of these canonical local heights in the non-archimedean case is the subject of Section 2.3 whose most important result is Proposition 2.14. Finally, we introduce three different methods for the computation of archimedean canonical local heights in Section 2.4.

Chapter 3. Jacobian surfaces

In this chapter we first review the general theory of Jacobian and Kummer surfaces in Section 3.1 and discuss known methods for the computation of canonical heights in Section 3.2 before introducing a new algorithm for the computation of canonical local heights at non-archimedean places in the remainder of the chapter. After generalizing the explicit theory of Kummer surfaces due to Flynn in Section 3.3, we develop the necessary theory for our algorithm in Section 3.4. We focus on how the canonical local height changes under a transformation of the given model and show that, after possibly a small and easily controlled field extension, we can always reduce to essentially five different types of reduction. In Section 3.5 we discuss how these types can be distinguished using certain invariants of curves of genus 2 called Igusa invariants before presenting formulas for the canonical local height in these cases in Section 3.6. Finally, we discuss the situation for archimedean places in Section 3.7. The simplification process presented in Section 3.4.4, the case distinction based on Igusa invariants given in Section 3.5 and the methods from Section 3.6 have been implemented in `Magma`.

Chapter 4. Jacobian threefolds

The objective of this chapter is to generalize as many concepts and results of the previous chapter as possible to the situation of a Jacobian threefold. It

turns out that even in the situation of the Jacobian of a hyperelliptic curve of genus 3 with a rational Weierstrass point at infinity several problems appear which we did not encounter in the situation of Jacobian surfaces. One obstacle is that the algebra is much more complicated than the algebra needed so far.

The first task is the explicit construction of the Kummer variety K associated to such a Jacobian J. Here we can build on earlier work by Stubbs [100] who constructs an embedding of K into $\mathbb{P}^7$; we review this embedding in Section 4.1. Next we find defining equations for the image of K under this embedding. One of the new phenomena is that there is a *quadratic* relation on K, whereas the Kummer surface is a *quartic* hypersurface. In Section 4.3 we discuss the traces which the group law on the Jacobian leaves on K using earlier work due to Duquesne [32]. In Chapter 3 these were given by certain biquadratic forms B_{ij} and quartic forms δ_i. We show that no such biquadratic forms can exist in genus 3, but conjecture, based on experimental evidence, that there are analogs of the δ_i.

Under the assumption that the conjecture is valid, we can immediately generalize several definitions and results from the previous chapter and we do so in Section 4.4. We discuss non-archimedean canonical local heights in Section 4.4.1, finding that some results can only be generalized under further assumptions, and the case of archimedean canonical local heights in Section 4.4.2. Here it turns out that their computation using theta functions given in Section 3.7.2 generalizes easily.

Chapter 5. Arithmetic intersection theory

In order to find an algorithm suitable for more general curves, we take a completely different approach in this chapter. It turns out that we can express the canonical height of a point on the Jacobian purely in terms of data on the curve using Theorem 5.11. This result allows us to write the canonical height as a sum of certain pairings, called local Néron symbols, between relatively prime divisors representing the point in question. In Section 5.1 we review the construction of these symbols using intersection theory on regular models of the curve and Green's functions on Riemann surfaces. Apart from the statement of Theorem 5.11, Section 5.2 also contains the basic outline of an algorithm for the computation of canonical heights consisting of six steps and a discussion of different ways of representing divisors.

These six steps are dealt with in the remainder of this chapter. We have to find out which places can lead to non-trivial intersection multiplicities; this can be done using Gröbner bases as in Section 5.3.2. The actual computations of the local Néron symbols are discussed in the remaining sections. We explain how intersection multiplicities on certain regular models can be computed using Gröbner bases over local rings in Section 5.3.4 and express the archimedean local Néron symbols in terms of (by now familiar) theta

functions on the Jacobian in Section 5.3.6. The relevant algorithms have been implemented in `Magma`.

Chapter 6. Examples and timings

This chapter is divided into two parts: The first part contains a discussion on how our algorithm for the computation of canonical heights and the bounds on the height constant discussed in Chapter 3 relate to the state of the art. The second part provides two examples where the canonical height algorithm developed in Chapter 5 is used. We also discuss its limitations and running time; this discussion is kept rather informal.

Appendix A. Proofs of some results from Chapter 3

Because some of the proofs in Chapter 3 are completely elementary, but very long and tedious, we have chosen to collect them in this Appendix. We hope that this will make it easier for the reader to concentrate on the main points of Chapter 3.

Chapter 1

Motivation and background

In this preparatory chapter all objects from algebraic or arithmetic geometry that we use without definition are defined and discussed in Chapter A of [49], in [65] or in [9]. We do not give any proofs for standard results, but instead refer to the above-mentioned literature.

1.1 Places and absolute values

We first set some notation. In this thesis k always denotes a number field or a function field of dimension one with fixed algebraic closure $\bar{k}$ and ring of integers $\mathcal{O}_k$. In the latter case we make no assumption on the characteristic of k, unless stated otherwise, but it will always be assumed that all residue fields are perfect. Let M_k denote the set of places of k and M_k^0 (respectively M_k^∞) the set of non-archimedean (respectively archimedean) places of k. If k is a function field, then M_k^∞ is empty.

For $v \in M_k^0$, let

$$v : k \longrightarrow \mathbb{Z} \cup \{\infty\}$$

denote the additive discrete valuation at v, normalized such that it is surjective.

If $v \in M_k$, then we can associate an absolute value $|.|_v$ to v in a non-unique way. We normalize $|.|_v$ for $v \in M_\mathbb{Q}$ by requiring $|p|_v = p^{-1}$ for a non-archimedean place v corresponding to a prime p and by setting $|a|_\infty = |a|$ for $a \in \mathbb{Q}$, where ∞ is the unique archimedean place of $\mathbb{Q}$ and $|.|$ is the usual absolute value. This gives rise to a normalization of absolute values on extensions of $\mathbb{Q}$. Namely, if $k/\mathbb{Q}$ is an extension and $v \in M_k$, then there is a unique place $v' \in M_\mathbb{Q}$ lying below v; we require that the restriction of $|.|_v$ to $\mathbb{Q}$ equals $|.|_{v'}$. In the case of a one-dimensional function field, we normalize our absolute values by requiring $|a|_v = \exp(-v(a))$ for any $a \in k$.

If $v \in M_k$ is a place of k, then we write k_v for the completion at v. If v is non-archimedean, then we denote the ring of integers of k_v by $\mathcal{O}_v$, its residue class field at v by $\mathfrak{k}_v$ and the cardinality of $\mathfrak{k}_v$ by q_v. We set N_v equal to $\log(q_v)$ if k is a number field and v is non-archimedean and to 1 in the other cases. Finally, we define for $v \in M_k$ the *local degree* n_v *at* v as the degree of the closed point corresponding to v if k is a function field and by $[k_v : \mathbb{Q}_{v'}]$ if k is a number field and $v' \in M_\mathbb{Q}$ such that v extends v'.

If $v \in M_k^0$, then we have

$$-n_v \log |a|_v = N_v v(a)$$

for any $a \in k_v^*$. For archimedean v we define

$$v(a) := -n_v \log |a|_v \text{ for } a \neq 0$$

and

$$v(0) = \infty.$$

The most important property which our fields satisfy is the product formula. It says that

$$\sum_{v \in M_k} -n_v \log |a|_v = \sum_{v \in M_k} N_v v(a) = 0 \text{ for all } a \in k^*. \tag{1.1}$$

For a proof of the product formula see [59, Chapter 2]. In addition we set $d_k = [k : \mathbb{Q}]$ in the number field and $d_k = 1$ in the function field case.

1.2 Heights on projective space, Weil heights and canonical heights

In this section we first define relative and absolute heights on projective space over number fields or one-dimensional function fields. These are functions taking values in the nonnegative real numbers that measure the size of a point. Then we define heights on projective varieties, focusing on abelian varieties, and finally canonical heights.

Definition 1.1. Let k be a number field or a one-dimensional function field and let $n \geq 1$ be an integer. Let $P = (x_0 : \ldots : x_n) \in \mathbb{P}^n_k$. Then the *(logarithmic) height of P relative to k* is

$$\begin{aligned} h_k(P) &:= \sum_{v \in M_k} -N_v \min\{v(x_0), \ldots, v(x_n)\} \\ &= \sum_{v \in M_k} n_v \max\{\log |x_0|_v, \ldots, \log |x_n|_v\}. \end{aligned}$$

Moreover, we call

$$h(P) := \frac{1}{d'_{k'}} h_{k'}(P)$$

the *absolute (logarithmic) height of P*, where k' is any field such that $P \in \mathbb{P}^n_{k'}$ and $d'_{k'}$ equals $d_{k'}$ if k is a number field and $[k' : k]$ if k is a function field.

Then [49, Lemma B.2.1] guarantees that $h(P)$ does not depend on the choice of k'.

Next we want to define heights on smooth projective varieties. The obvious idea is to choose an embedding into projective space and define the height on the variety to be the height on the image of the embedding. Such embeddings correspond to very ample divisors on the variety.

More generally, let k be a number field or a one-dimensional function field with fixed algebraic closure $\bar{k}$ and let V/k be a smooth projective variety defined over k. Let $\mathrm{Div}(V)$ denote the group of divisors on V and $\mathrm{Pic}(V)$ the Picard group. We also need the subgroups $\mathrm{Div}(V)(k')$ and $\mathrm{Pic}(V)(k')$

of k'-rational elements of $\mathrm{Div}(V)$ and $\mathrm{Pic}(V)$, respectively, where k' is an extension of k with algebraic closure $\bar{k}'$. These are the elements fixed by the Galois group $\mathrm{Gal}(\bar{k}'/k')$. If $f \in k(V)^*$, the we denote the principal divisor associated to f by $\mathrm{div}(f)$.

There is an association, in fact a homomorphism, that is known as *Weil's height machine* and is constructed as follows:

$$\mathrm{Div}(V) \longrightarrow \mathrm{Pic}(V) \longrightarrow \frac{\{h : V(\bar{k}) \to \mathbb{R}\}}{\{h : V(\bar{k}) \to \mathbb{R} \text{ bounded}\}}$$

Here we write a divisor $D \in \mathrm{Div}(V)$ as the difference $D = D_1 - D_2$ of two very ample divisors with associated embeddings ϕ_1 and ϕ_2, respectively, and set

$$h_{V,D}(P) := h(\phi_1(P)) - h(\phi_2(P))$$

for all $P \in V(\bar{k})$. We associate to D the class $[h_{V,D}]$ in $\frac{\{h:V(\bar{k})\to\mathbb{R}\}}{\{h:V(\bar{k})\to\mathbb{R} \text{ bounded}\}}$. See [49, Theorem B.3.2] for a proof of the fact that this is a well-defined homomorphism and of several other properties. In particular Weil's height machine is functorial in the sense that if we have a morphism $\phi : V \longrightarrow V'$ of smooth projective varieties defined over k and $D' \in \mathrm{Div}(D')$, then

$$[h_{V,\phi^*(D')}] = [h_{V',D'} \circ \phi].$$

Suppose now that we have a morphism $\phi : V \longrightarrow V$ and a divisor $D \in \mathrm{Div}(V)$ such that $\phi^*([D]) = d[D]$, where $[D]$ is the linear equivalence class of D and $d > 1$. Then the sequence $\big(d^{-n} h_D\big(\phi^n(P)\big)\big)_n$ converges as n approaches infinity and we define

$$\hat{h}_{\phi,D}(P) := \lim_{n\to\infty} d^{-n} h_D\big(\phi^n(P)\big)$$

and obtain a height function associated to the class $[D]$ satisfying

$$\hat{h}_{\phi,D}(\phi(P)) = d\hat{h}_{\phi,D}(P)\,.$$

We call $\hat{h}_{\phi,D}$ the *canonical height on V with respect to ϕ and D*.

In the special case where $V = A$ is an abelian variety defined over k, there is a natural morphism to choose, namely the duplication map $[2] : A \longrightarrow A$. Recall that if $[D]$ is an ample symmetric divisor class on A, then we have $[2]^*([D]) = 4[D]$.

Definition 1.2. Let k be a number field or a one-dimensional function field and A/k an abelian variety defined over k. Let $D \in \mathrm{Div}(A)$ such that $[D] \in \mathrm{Pic}(A)$ is ample and symmetric. The function

$$\hat{h}_D := \hat{h}_{[2],D}$$

is called the *canonical height* or *Néron-Tate height on A with respect to D*.

The most important properties of the canonical height are summarized in the following theorem. We denote for any group G the subgroup of elements of G of finite order by G_{tors}. Furthermore, if $n \in \mathbb{Z}$ and $P \in A$ is a point on an abelian variety, then we abbreviate $[n](P)$ by nP.

Theorem 1.3. *(Néron, Tate) Let k be a number field or a one-dimensional function field and A/k an abelian variety defined over k. Let $D \in \mathrm{Div}(A)$ such that $[D] \in \mathrm{Pic}(A)$ is ample and symmetric. The following are satisfied:*

(i) $\hat{h}_D(mP) = m^2 \hat{h}_D(P)$ *for all* $m \in \mathbb{Z}, P \in A(\bar{k})$

(ii) $\hat{h}_D(P+Q) + \hat{h}_D(P-Q) = 2\hat{h}_D(P) + 2\hat{h}_D(Q)$ *for all* $P, Q \in A(\bar{k})$

Now suppose that k is a number field.

(iii) $\hat{h}_D(P) \geq 0$ *for all* $P \in A(\bar{k})$ *and* $\hat{h}_D(P) = 0$ *if and only if* $P \in A(\bar{k})_{\text{tors}}$.

(iv) $\hat{h}_D : A(\bar{k})/A(\bar{k})_{\text{tors}} \longrightarrow \mathbb{R}$ *is a positive definite quadratic form that extends $\mathbb{R}$-linearly to a positive quadratic form on $A(\bar{k}) \otimes \mathbb{R}$.*

(v) *The set $\{P \in A(k') : \hat{h}_D(P) \leq B\}$ is finite for every number field k' over which A is defined and every bound B.*

Proof. See [49, §B.5]. □

1.3 Néron functions

In this thesis we are interested in practical methods to compute canonical heights on certain abelian varieties. However, it is not a very good idea to use Definition 1.2 for this purpose, since the size of the coordinates that we need to compute - assuming we can represent them somehow - grows exponentially. Fortunately, there are other methods. The definition of the canonical height given in the previous section is due to Tate, but at the same time Néron constructed the canonical height as the sum of local contributions in [78]. It was later reformulated in the language we use below by Lang, see [59, Chapter 11]. Although the construction is more complicated than Tate's construction, which allows for a rather short proof of Theorem 1.3, it has both theoretical and practical merits. We shall split the canonical height into a sum of certain functions which Lang calls Néron functions and Hindry-Silverman call canonical local heights. We shall see that this decomposition allows us to compute canonical heights for abelian varieties of dimension one and two.

Let A be an abelian variety defined over a field l with an absolute value v. Let $D \in \mathrm{Div}(A)(l)$.

Definition 1.4. A *Weil function associated with D and v* is a function

$$\lambda_{D,v} : A(l) \setminus \mathrm{supp}(D) \longrightarrow \mathbb{R}$$

with the following property: Suppose D is represented locally by (U, f), where $U \subset A(l)$ is an open subset and f is a rational function. Then there exists a locally bounded continuous function $\alpha : U \longrightarrow \mathbb{R}$ such that for all $P \in U \setminus \mathrm{supp}(D)$ we have

$$\lambda_{D,v}(P) = -\log |f(P)|_v + \alpha(P),$$

where the normalization of $|.|_v$ has been fixed in Section 1.1.

In this context, 'locally bounded' means bounded on bounded subsets and 'bounded' and 'continuous' refer to the v-adic topology, see [59, §10.1].

Next we define Néron functions, which are Weil functions having some special properties.

Definition 1.5. We call an association $D \mapsto \lambda_D$ associating to each l-rational divisor D on A a Weil function λ_D a *Néron family* if the following conditions are satisfied.

(1) If $D, E \in \mathrm{Div}(A)(l)$, then $\lambda_{D+E,v} = \lambda_{D,v} + \lambda_{E,v} + c_1$ for some $c_1 \in \mathbb{R}$.

(2) If $D = \mathrm{div}(f) \in \mathrm{Div}(A)(l)$ is principal, then $\lambda_{D,v} = -\log |f|_v + c_2$ for some $c_2 \in \mathbb{R}$.

(3) For all $D \in \mathrm{Div}(A)(l)$ we have $\lambda_{[2]^*(D),v} = \lambda_{D,v} \circ [2] + c_3$ for some $c_3 \in \mathbb{R}$.

We call the image $\lambda_{D,v}$ under such an association a *Néron function associated with D and v*.

Lang shows in [59, §11.1] that for any l-rational divisor D on an abelian variety A there exists a Néron function $\lambda_{D,v}$ associated with D and v that is unique up to constants. In the process he shows how Néron functions can be constructed. This also gives a method of verifying whether a given Weil function associated with a divisor on an abelian variety is a Néron function when the linear equivalence class of the divisor is symmetric.

Proposition 1.6. *(Lang) Let $D \in \mathrm{Div}(A)(l)$ be a divisor whose class in $\mathrm{Pic}(A)$ is symmetric and let λ be a Weil function associated with D and v. Let $f \in l(A)$ be a rational function such that $[2]^*(D) = 4D + \mathrm{div}(f)$, and let $\varepsilon : A(l) \longrightarrow \mathbb{R}$ be the unique bounded continuous function on $A(l)$ such that*

$$\lambda(2P) = 4\lambda(P) - \log |f(P)|_v - \varepsilon(P)$$

for all P outside a suitable Zariski closed subset of $A(l)$.

Let $\mu(P) := \sum_{n=0}^{\infty} 4^{-n-1}\varepsilon(2^n P)$ *and let* $\hat{\lambda} := \lambda - \mu$. *Then* $\mu : A(l) \longrightarrow \mathbb{R}$ *is bounded and continuous. Furthermore,* $\hat{\lambda}$ *is the unique Néron function associated with* D *and* v *that satisfies*

$$\hat{\lambda}(2P) = 4\hat{\lambda}(P) - \log|f(P)|_v. \tag{1.2}$$

Proof. A similar result is proved in [59, Chapter 11, Proposition 1.1]. The following proof is a generalization of the discussion preceding [43, Theorem 4].

Existence and uniqueness of ε are obvious because λ is a Weil function. Note that although λ is only defined on $A(l) \setminus \mathrm{supp}(D)$, the function ε is defined on all of $A(l)$, because it is a Weil function associated with $0 \in \mathrm{Div}(A)$ and v. See Proposition 2.3 and Corollary 2.4 of [59, Chapter 10].

It follows from this that μ converges and is defined on $A(l)$. It is also bounded and continuous, since multiplication by 2^n is continuous. A straightforward calculation reveals that we have

$$\varepsilon(P) = 4\mu(P) - \mu(2P);$$

this is known as Tate's telescoping trick.

Hence we get

$$\begin{aligned}\hat{\lambda}(2P) - 4\hat{\lambda}(P) &= \lambda(2P) - \mu(2P) - 4\lambda(P) + 4\mu(P)\\ &= -\log|f(P)|_v.\end{aligned}$$

Therefore $\hat{\lambda}$ satisfies property (3) of a Néron function. The verifications that it also satisfies (1) and (2) are immediate; this proves the Proposition. □

In particular it follows that any Weil function satisfying (1.2) will automatically be a Néron function. The crucial point is that we can fix a specific Néron function in its class modulo constants by fixing the function f.

Definition 1.7. Let $f \in l(A)$ be a rational function such that $[2]^*(D) = 4D + \mathrm{div}(f)$. We call the unique Néron function that satisfies (1.2) the *canonical local height on* A *associated with* D, v *and* f and denote it by $\hat{\lambda}_{D,v,f}$.

We now relate canonical local heights to canonical heights. The following theorem tells us that if we pick some f as above consistently for all places v, then the sum of all canonical local heights associated with D and f coincides with the canonical height.

Theorem 1.8. *(Néron) Let* k *be a number field or a one-dimensional function field and let* A *be an abelian variety defined over* k. *Let* D *be a* k*-rational*

divisor on A whose class is ample and symmetric and let $f \in k(A)$ be a rational function such that $[2]^*(D) = 4D + \mathrm{div}(f)$. For each $v \in M_k$ let $\hat{\lambda}_{D,v,f}$ denote the canonical local height associated with D, v and f. Then we have

$$\hat{h}_D(P) = \frac{1}{d_k} \sum_{v \in M_k} n_v \hat{\lambda}_{D,v,f}(P)$$

for all $P \in A(k) \setminus \mathrm{supp}(D)$.

Proof. Although this theorem is not proved there directly in this form, it follows almost immediately from the results of [59, §11.1]. □

It is worth noting that when the condition $P \notin \mathrm{supp}(D)$ fails we can repair the situation easily; we can use the moving lemma (cf. [49, Lemma A.2.2.5 (ii)]) to find some $D' \in [D]$ such that $P \notin \mathrm{supp}(D')$ and use suitable canonical local heights for D'.

Remark 1.9. The canonical local heights are defined not only on $A(k)$, but also on $A(k_v)$. Therefore we may and shall pass to the completion whenever we only deal with one place at a time.

Remark 1.10. We have not defined canonical heights for anti-symmetric divisor classes $[D]$. This is possible, but leads to a linear form, as opposed to a quadratic form. It can also be decomposed into a sum of canonical local height and the only difference is that we have to take a function f satisfying $[2]^*D = 2D + \mathrm{div}(f)$ in the preceding theorem. It is also possible to construct canonical heights for general divisors on A as a sum of a quadratic and a linear form. All of this is done in [49, §B.5].

Remark 1.11. For an exposition of canonical local heights in terms of line bundles see [8, Chapter 9].

1.4 Néron models

In this section we study the interplay between Néron functions associated to a non-archimedean place v and the Néron model of A over the spectrum of the ring of integers $\mathcal{O}_v$ of the completion k_v of k at v. Our main references are [9] and [59].

Let R denote a Dedekind domain with field of fractions l and let $S = \mathrm{Spec}(R)$.

Definition 1.12. Let V be a smooth projective variety over l of dimension d. We call a closed subscheme in some $\mathbb{P}^n_l$ given by a set of defining equations of V in $\mathbb{P}^n_l$ a *model of V over* $\mathrm{Spec}(l)$ and we say that the model is *R-integral* if the equations have coefficients in R. If M is an R-integral model of V over

Spec(l), then we call the closed subscheme of $\mathbb{P}^n_R$ defined by the equations in M the *closure of M over S*.

Moreover, we define a *model of V over S* to be a normal and flat S-scheme $\mathcal{V} \to S$ of dimension $d+1$ together with an isomorphism $\mathcal{V}_l \cong V$, where $\mathcal{V}_l$ is the generic fiber of $\mathcal{V}$. For each closed $v \in S$ we denote the special fiber of $\mathcal{V}$ above v by $\mathcal{V}_v$.

Remark 1.13. If M is a model of a smooth projective variety V over Spec(l), then we usually call M a *model of V* without mentioning Spec(l) explicitly. Moreover, we will regularly abuse notation by using V for both the variety and its given model, and talk about the closure of V when we mean in fact the closure of the given (R-integral) model of V over S, unless this might cause confusion. Conversely, we always mention the base scheme S when we talk about a model of a variety V over S.

Note that if the closure of a given R-integral model of V is normal and flat, then it is a model of V over S.

We are especially interested in models which are proper and regular. However, if $V = A$ is an abelian variety, then it is natural to look for models of A over S which are regular (or even smooth over S), but also retain as much of the group structure of A as possible. It turns out that in general it is not possible to find such a model if we also require properness, but Néron found a way to construct a model that satisfies a property which suffices in applications.

Definition 1.14. Let A be an abelian variety defined over l. A *Néron model of A over S* is a separated scheme $\mathcal{A} \longrightarrow S$ with generic fiber $\mathcal{A}_l$ isomorphic to A that is smooth over S and satisfies the following universal property: If $\mathcal{X} \longrightarrow S$ is a smooth S-scheme with generic fiber $\mathcal{X}_l$, then any morphism $\phi : \mathcal{X}_l \longrightarrow \mathcal{A}_l$ extends uniquely to a morphism $\mathcal{X} \longrightarrow \mathcal{A}$ over S.

In particular, the uniqueness property guarantees that any l-rational point corresponds to a section in $\mathcal{A}(S)$. Although this is weaker than properness, it suffices for most purposes. The next result states that Néron models exist and that they have a structure which is as close to the group structure on A as possible.

Theorem 1.15. *(Néron) Let A be an abelian variety defined over l. Then there exists a Néron model $\mathcal{A} \longrightarrow S$ of A. It is a group scheme over S whose group scheme structure extends the* Spec(l)*-group scheme structure on A. Moreover it is unique up to unique isomorphism.*

Proof. The original proof is very deep and can be found in [77]. For a more modern proof see [9]. □

We only use Néron models locally, so we might as well restrict to the case where R is a discrete valuation ring with field of fractions l, valuation

v and residue field $\mathfrak{l}$. Let $S = \mathrm{Spec}(R)$. Let $\mathcal{A}$ be the Néron model of A over S and let $\mathcal{A}_l$ and $\mathcal{A}_v$ be its generic and special fiber, that is the fibers lying over the generic point and the special point $v \in \mathrm{Spec}(\mathcal{O}_v)$, respectively. In particular $\mathcal{A}_l$ is isomorphic to A.

It is shown in [9, §6.5, Corollary 3] that $\mathcal{A}$ is also the Néron model of A over $\mathrm{Spec}(R^{\mathrm{sh}})$, where R^{sh} is the strict henselization of R, with field of fractions l^{sh}. The advantage of working over $\mathrm{Spec}(R^{\mathrm{sh}})$ is that the residue field of R^{sh} is separably closed.

Definition 1.16. Suppose the special fiber $\mathcal{A}_v$ has irreducible components $\mathcal{A}_v^0, \dots \mathcal{A}_v^n$, where n is a nonnegative integer and $\mathcal{A}_v^0$ is the connected component of the identity of $\mathcal{A}_v$. The *group of components* Φ_v *of* $\mathcal{A}_v$ is defined by

$$\Phi_v := \mathcal{A}_v / \mathcal{A}_v^0.$$

The nonnegative integer $c_v := \#\Phi_v(\mathfrak{l})$ is called the *Tamagawa number of* A/l. Furthermore, the *identity component* $\mathcal{A}^0$ *of* $\mathcal{A}$ is defined as the open subscheme of $\mathcal{A}$ with generic fiber A and special fiber $\mathcal{A}_v^0$. We define A_0 to be the subset of A of points mapping to the connected component $\mathcal{A}_v^0$.

Note that $\mathcal{A}_v^0$ is always defined over $\mathfrak{l}$. Because of the group scheme structure A_0 is a subgroup of A and we have

$$\Phi_v \cong A(l^{\mathrm{sh}}) / A_0(l^{\mathrm{sh}})$$

and

$$\Phi_v(\mathfrak{l}) \cong \left(A(l^{\mathrm{sh}}) / A_0(l^{\mathrm{sh}}) \right)^{\mathrm{Gal}(l^{\mathrm{sh}}/l)} \cong A(l)/A_0(l).$$

The last isomorphism is not obvious, but follows from $A_0(l^{\mathrm{sh}})^{\mathrm{Gal}(l^{\mathrm{sh}}/l)} = A_0(l)$ and the vanishing of $H^1\left(\mathrm{Gal}(l^{\mathrm{sh}}/l), A_0(l^{\mathrm{sh}})\right)$. The latter statement is part of the proof of [72, Chapter 1, Proposition 3.8].

If $P \in \mathcal{A}_l$ is an l-rational point on the generic fiber, then, by the universal property of the Néron model, this point is the image of the generic point of S under a section $\sigma_P : S \longrightarrow \mathcal{A}$ and the image of the special point $v \in S$ lies in one of the components of the special fiber. Let $D \in \mathrm{Div}(A)(l)$ be a prime divisor. We write its Zariski closure on $\mathcal{A}$ as $D_{\mathcal{A}}$; this is a prime divisor on $\mathcal{A}$ and if P does not lie in the support of D, then pulling this divisor back to S gives

$$\sigma_P^*(D_{\mathcal{A}}) = i(D, P)(v) \in \mathrm{Div}(S) \tag{1.3}$$

for some well-defined integer $i(D, P)$, because any divisor on S is an integral multiple of the special point v. We call $i(D, P)$ the *intersection multiplicity of* D *and* P *at* v. This construction can be extended to arbitrary $D \in \mathrm{Div}(A)(l)$ by linearity. In general this is not an intersection multiplicity in the usual sense, since the Néron model might not be proper and hence one would need a completion satisfying certain properties in order to construct

a reasonable intersection theory on it. Such a completion is not known to exist in general, but see the proof of Proposition 2.14 below for the elliptic curve case. Also see [59, §12.3] for a discussion of this issue.

We can compute $i(D, P)$ using the following observation: If $D_{\mathcal{A}}$ is represented by $f \in l(\mathcal{A}) = l(\mathcal{A}_l)$ around $\sigma_P(v)$, then we have

$$i(D, P) = v(f(P)), \tag{1.4}$$

and this does not depend on the choice of f. For the next theorem we specialize R further to the rings that we are interested in.

Theorem 1.17. *(Néron, Lang) Let k_v be the completion of a number field or a one-dimensional function field at a non-archimedean place v with ring of integers $\mathcal{O}_v$. Let A be an abelian variety defined over k_v and let $\mathcal{A}$ be its Néron model over* $\mathrm{Spec}(\mathcal{O}_v)$*. Let $D \in \mathrm{Div}(A)(k_v)$ and let $\lambda_{D,v}$ be a Néron function associated with D and v.*

For each component $\mathcal{A}_v^j$ there is a constant $\gamma_j(D) \in \mathbb{Q}$ such that for all

$$P \in A(k_v) \setminus \mathrm{supp}(D)$$

mapping to $\mathcal{A}_v^j$ we have

$$\lambda_{D,v}(P) = \frac{N_v}{n_v}(i(D, P) + \gamma_j(D)).$$

Proof. See [59, Chapter 11, Theorem 5.1]. □

The preceding theorem shows that the canonical height on an abelian variety is intimately related to intersection multiplicities on the corresponding Néron models over the rings of integers of the completions. Indeed, Néron's original construction used these intersection multiplicities, mainly developed by Néron himself, in a crucial way. It is possible to say more about the possible denominators of $\gamma_j(D)$; this is done by Lang in [59, Chapter 11, Theorem 5.2].

1.5 Curves and Jacobians

In this section we restrict to those abelian varieties that are of special interest to us, namely Jacobians of smooth projective curves. It turns out (see Theorem 1.36) that in this case the Néron model, which was defined using an abstract uniqueness property, can be described more concretely in terms of certain models of the underlying curve, to be defined below. For this we discuss several concepts that will also be of great importance later on, notably in Chapter 5. For proofs and more elaborate discussions we will mostly refer to the books [65], [25] and [9]. For now we return to the general situation where R is a Dedekind domain with field of fractions l and spectrum S.

Definition 1.18. An *arithmetic surface over* S is an integral, projective, normal and flat S-scheme of dimension 2 such that its generic fiber is a smooth projective curve over l.

Arithmetic surfaces are analogs of normal fibered surfaces over a smooth projective curve defined over an algebraically closed field, with the base curve replaced by the arithmetic curve S. As is the case for fibered surfaces, any prime divisor D on an arithmetic surface $\chi : \mathcal{C} \longrightarrow S$ is either horizontal or vertical. Here a divisor $D \in \mathrm{Div}(\mathcal{C})$ is called *horizontal* if $\chi(D) = S$ and it is called *vertical* or *fibral*, if $\chi(D)$ is a point. For each closed $v \in S$ we let $\mathrm{Div}_v(\mathcal{C})$ denote the subgroup of v-vertical divisors, that is formal linear combinations of the irreducible components of the special fiber $\mathcal{C}_v$.

For the remainder of this section, let C denote a smooth projective geometrically connected curve over l of genus g, given by an R-integral model. If it is normal and flat, then the closure (more precisely, the closure of the given model, see Remark 1.13) of C over S is an arithmetic surface that is a proper model of C over S, although it is not regular in general. But its special fibers are geometrically connected, since C is, see [65, Chapter 8, Corollary 3.6]. One way to obtain a proper regular model is to start with the closure of C over S and try to resolve its singularities without changing the generic fiber.

Definition 1.19. Let X denote a reduced locally Noetherian scheme. A proper birational morphism $\xi : X' \to X$ with X' regular is called a *desingularization of* X. If ξ is an isomorphism above every regular point of X, then ξ is a *desingularization of* X *in the strong sense*. We say that ξ is a *minimal desingularization of* X if any other desingularization of X factors uniquely through ξ. If it exists, a minimal desingularization is unique up to unique isomorphism.

The following theorem says that if we start with the closure $\mathcal{C}$ of C over S, then we can always compute a desingularization of $\mathcal{C}$ in the strong sense which is necessarily a proper regular model of C over S.

Theorem 1.20. *(Lipman) Let $\mathcal{C} \to S$ be a 2-dimensional integral, projective flat S-scheme and define a sequence*

$$\cdots \longrightarrow \mathcal{C}_{i+1} \longrightarrow \mathcal{C}_i \longrightarrow \cdots \longrightarrow \mathcal{C}_1 \longrightarrow \mathcal{C}_0 = \mathcal{C} \tag{1.5}$$

as follows: $\mathcal{C}_1 \longrightarrow \mathcal{C}_0$ is the normalization of $\mathcal{C}$ and for each $i \geq 1$ we let

$$\mathcal{C}_{i+1} \longrightarrow \mathcal{C}_i$$

denote the normalization of the blow-up of $\mathcal{C}_i$ along the (necessarily finite) singular locus of $\mathcal{C}_i$. Then there exists some $N \geq 0$ such that $\mathcal{C}_N$ is regular. In particular, $\mathcal{C}_N$ is a desingularization of $\mathcal{C}$ in the strong sense.

Proof. See [3], where $\mathcal{C}$ is assumed to be excellent. This condition can be eliminated a posteriori as in [65, Chapter 8, Corollary 3.51]. □

The computation of proper regular models using Theorem 1.20 is implemented in `Magma` [67] by Donnelly, at least when l is the completion of a number field or a one-dimensional function field at a non-archimedean place. See Section 5.3.3.

The blow-ups alluded to in Theorem 1.20 are easy and we will see several examples later on. See [89, §IV.7] for a practical introduction and more examples. In contrast, normalizations are usually much more difficult and so it is a natural question when the need for them does not occur.

Definition 1.21. Let $\mathcal{C} \longrightarrow S$ be an arithmetic surface and let $\xi : \mathcal{C}' \longrightarrow \mathcal{C}$ be a desingularization of $\mathcal{C}$. We say that $\mathcal{C}$ has *rational singularities* if $R^i\xi_*\mathcal{O}_{\mathcal{C}'}$ vanishes for all $i > 0$, where $\mathcal{O}_{\mathcal{C}'}$ is the structure sheaf of $\mathcal{C}'$.

Remark 1.22. The condition on the vanishing of the higher direct images is independent of the desingularization.

Example 1.23. Regular arithmetic surfaces have rational singularities. More generally, arithmetic surfaces whose only singularities are ordinary double points have rational singularities, so in particular semistable models have rational singularities.

Lemma 1.24. *(Lipman, Mattuck) Suppose that $\mathcal{C} \longrightarrow S$ is an arithmetic surface with rational singularities and that $\xi : \mathcal{C}' \longrightarrow \mathcal{C}$ is the blow-up of $\mathcal{C}$ along a singular point $P \in \mathcal{C}$. Then $\mathcal{C}'$ is normal and has rational singularities.*

Proof. See [3]. □

Corollary 1.25. *Suppose $\mathcal{C} \longrightarrow S$ is an arithmetic surface with rational singularities. Then no normalizations are necessary in order to compute a desingularization of $\mathcal{C}$ in the strong sense using Theorem 1.20.*

It will be important for us to characterize those cases when the closure $\mathcal{C}$ of C over S has rational singularities. Unfortunately the author is not aware of any method of doing so without first computing a desingularization of $\mathcal{C}$.

Lemma 1.26. *(Artin) Let $\mathcal{C} \longrightarrow S$ be an arithmetic surface with singular points $P_1, \ldots, P_n \in \mathcal{C}$. Let $\xi : \mathcal{C}' \longrightarrow \mathcal{C}$ be a desingularization of $\mathcal{C}$. For each $i \in \{1, \ldots, n\}$ let Y_i denote the preimage of P_i under ξ, with irreducible components $Y_{i,1}, \ldots, Y_{i,m_i}$.*

Then $\mathcal{C}$ has rational singularities if and only if we have $p_a(Z_i) \leq 0$ for each $Z_i = \sum_{j=1}^{m_i} a_j Y_{i,j} \in \mathrm{Div}_v(\mathcal{C}')$, where the a_j are nonnegative integers and $p_a(Z_i)$ is the arithmetic genus of Z_i.

Proof. See [2, Proposition 1]. □

Remark 1.27. This result can be improved as follows. Let Z_i denote the fundamental cycle of Y_i, defined in [2]. Then $\mathcal{C}$ has rational singularities if and only if $p_a(Z_i) = 0$ for all $i \in \{1, \ldots, n\}$. See [2, Theorem 3].

If $\mathcal{C}$ is any model of C over S, then the minimal desingularization of $\mathcal{C}$ introduced in Definition 1.19 depends on $\mathcal{C}$. There exists a different notion of minimality that only depends on C.

Theorem 1.28. *(Lichtenbaum, Shafarevich) Suppose that $g \geq 1$. There exists a proper regular model $\mathcal{C}^{\min}$ of C over S, unique up to unique S-isomorphism, such that if $\mathcal{C}$ is another proper regular model of C over S, then any isomorphism from $\mathcal{C}_l$ to $\mathcal{C}_l^{\min}$ induces an S-morphism $\mathcal{C} \longrightarrow \mathcal{C}^{\min}$. We call $\mathcal{C}^{\min}$ the* minimal proper regular model of C. *It is unique up to unique isomorphism.*

Proof. See [21, Theorem 1.2]. □

From now on we assume that $g \geq 1$. In order to state Proposition 1.31, which explains how the minimal proper regular model is characterized and how it can be computed, we need to introduce intersection theory on (regular) arithmetic surfaces. This will figure more prominently in Chapter 5. Let $\chi : \mathcal{C}' \longrightarrow S$ be a regular model of C over S.

In the following we will need lengths of modules. If A is a commutative ring and M is an Artinian and Noetherian A-module, then we denote by $\text{length}_A(M)$ the length of M as an A-module, that is the length of a longest chain of non-trivial sub A-modules of M. Because of the assumptions on M this is always a well-defined nonnegative integer.

For simplicity we now restrict to the case that R is a discrete valuation ring with valuation v. Let $\pi = \pi_v$ be a uniformiser and let $\mathfrak{l}$ denote the residue field. We want to intersect divisors in $\text{Div}(\mathcal{C}')$.

Definition 1.29. Let D, E be two effective divisors on $\mathcal{C}'$ without common component and let $P \in \mathcal{C}'_v$ be a closed point. Let $I_{D,P}$ and $I_{E,P}$ be defining ideals of D and E, respectively, in the local ring $\mathcal{O}_{\mathcal{C}',P}$. Then the integer

$$i_P(D, E) := \text{length}_{\mathcal{O}_{\mathcal{C}',P}} \left(\mathcal{O}_{\mathcal{C}',P} / (I_{D,P} + I_{E,P}) \right)$$

is called the *intersection multiplicity of D and E at P*. The *total intersection multiplicity of D and E* is

$$i_v(D, E) := \sum_P i_P(D, E)[\mathfrak{l}(P) : \mathfrak{l}],$$

where the sum is over all closed points $P \in \mathcal{C}'_v$.

Finally, we extend i_P and i_v by linearity to divisors $D, E \in \text{Div}(\mathcal{C}')$ without common component.

The intersection multiplicity is symmetric and bilinear, cf. [65, Chapter 9, Lemma 1.4]. In analogy with algebraic surfaces we would like to define self-intersections of divisors. However, intersections as defined above do not respect linear equivalence, and so the usual idea, namely to use the moving lemma, does not work in this case. This was in fact the basic problem which motivated the development of Arakelov intersection theory, see Remark 5.13. But if we restrict to fibral divisors, then we have the following result:

Lemma 1.30. *Let $D \in \mathrm{Div}_v(\mathcal{C}')$. Then we have*

$$i_v(D, \mathrm{div}(f)) = 0$$

for any $f \in l(\mathcal{C}'_v)^*$. There exists some $f \in l(\mathcal{C}'_v)^*$ such that $\mathrm{supp}(D) \cap \mathrm{supp}(D + \mathrm{div}(f)) = \emptyset$ and we can define the self-intersection $i_v(D, D)$ by

$$i_v(D, D) := i_v(D, D + \mathrm{div}(f)).$$

We have $i_v(D, D) \leq 0$ and the following are equivalent:

(a) $i_v(D, D) = 0$.

(b) D is orthogonal to $\mathrm{Div}_v(\mathcal{C}')$ with respect to $i_v(\cdot, \cdot)$.

(c) $D = q\mathcal{C}'_v$ for some $q \in \mathbb{Q}$.

Proof. See any one of [65, §9.1.2], [60, III, Proposition 3.5], or [89, IV, Proposition 7.3]. □

Now we can return to our discussion of minimal proper regular models. If the residue field is algebraically closed, then we say that a vertical divisor $D \in \mathrm{Div}_v(\mathcal{C})$ on a special fiber of an arithmetic surface is *exceptional* if it is isomorphic to $\mathbb{P}^1$ and has self-intersection equal to -1. Otherwise rationality questions have to be taken into account. For a precise formulation see [65, §9.3.1].

Proposition 1.31. *(Castelnuovo's criterion) A proper regular model of C over S is minimal if and only if it contains no exceptional divisors.*

Proof. See [21, Theorem 3.1]. □

So in order to construct the minimal proper regular model of C over S, we first compute a desingularization of the closure of C over S and then contract exceptional divisors until none are left.

We now look at two very similar examples illustrating some of the concepts introduced in this section. See also [65, §10.1.1] for other interesting examples.

Example 1.32. Let $p > 3$ be a prime number and let E be the elliptic curve defined over $\mathbb{Q}_p$ that is given by the equation

$$y^2 = x^3 + p^6.$$

This equation is $\mathbb{Z}_p$-integral, but clearly not p-minimal.

Let $\mathcal{C}$ denote the closure of the given model of E over $S = \mathrm{Spec}(\mathbb{Z}_p)$. We first compute a desingularization of $\mathcal{C}$ using Theorem 1.20 and then contract exceptional components to find $\mathcal{C}^{\min}$, see Figure 1.1. We shall treat $\pi = p$ as a variable and write $x = x_i\pi^i$ and $y = y_i\pi^i$ for any i. We first blow up the singular point $(x, y, \pi) = (0, 0, 0)$. This yields three affine charts; we only list two since the third reveals no new information.

Chart 1: We use $(x, y, \pi) \mapsto (x_1, y_1, \pi)$. This yields

$$y_1^2 = \pi(x_1^3 + \pi^3),$$

which is normal with special fiber

$$\pi = 0, \quad y_1^2 = 0.$$

So we get an affine part of a double line that we denote by D. The only irregular point is $(x_1, y_1, \pi) = (0, 0, 0)$.

Chart 2: In this chart we use $(x, y, \pi) \mapsto (x, y', \pi')$, where $y' = y/x$ and $\pi' = \pi/x$, which leads to

$$y'^2 = x(1 + \pi'^3 x^3), \quad \pi = x\pi'.$$

This chart is normal and has special fiber

$$\begin{aligned} x = 0, &\quad y'^2 = 0, \\ \pi' = 0, &\quad y'^2 = x. \end{aligned}$$

Hence there are two components: Another affine part of the double line D and an affine part of a simple line A, both regular and intersecting transversally. The missing point of A is regular and lies in the third affine chart; in fact A is the strict transform of the nonsingular part of $\mathcal{C}_v$.

We need to blow up the singularity on the first affine chart.

Chart 1: We apply $(x_1, y_1, \pi) \mapsto (x_2, y_2, \pi)$ and obtain

$$y_2^2 = \pi^2(x_2^3 + 1),$$

which is not normal. In order to normalize, we replace y_2 by y_3 and get

$$y_3^2 = x_2^3 + 1.$$

The reduction of this is a smooth curve B of genus 1, intersecting D transversally. Hence we have computed a desingularization $\mathcal{C}'$ of $\mathcal{C}$ in the strong sense.

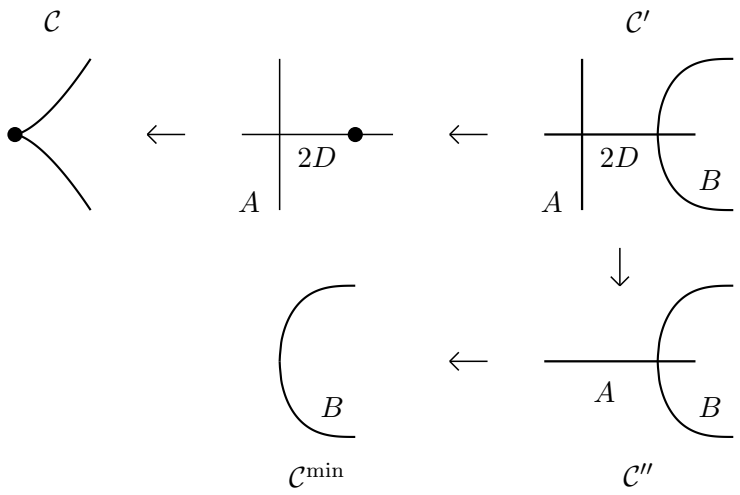

Figure 1.1: Models of $E : y^2 = x^3 + p^6$ over S

But this desingularization is not a minimal desingularization of $\mathcal{C}$. Consider the intersection matrix of $\mathcal{C}_v$, where the self-intersections are computed using Lemma 1.30.

$$\begin{pmatrix} i_p(A,A) & i_p(A,B) & i_p(A,D) \\ i_p(B,A) & i_p(B,B) & i_p(B,D) \\ i_p(D,A) & i_p(D,B) & i_p(D,D) \end{pmatrix} = \begin{pmatrix} -2 & 0 & 1 \\ 0 & -2 & 1 \\ 1 & 1 & -1 \end{pmatrix}$$

Hence D is exceptional and we can contract it to find another desingularization $\mathcal{C}''$ of $\mathcal{C}$ with intersection matrix

$$\begin{pmatrix} i_p(A,A) & i_p(A,B) \\ i_p(B,A) & i_p(B,B) \end{pmatrix} = \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}.$$

So we see that $\mathcal{C}''$ is the minimal desingularization of $\mathcal{C}$ since the only exceptional divisor left is A which is the strict transform of the nonsingular part of $\mathcal{C}_v$. However, the special fiber of the minimal proper regular model $\mathcal{C}^{\min}$ of E over S is equal to B and we get it by contracting A.

Note that in this example we had to normalize and accordingly $\mathcal{C}$ cannot have rational singularities. However, we performed the normalization step by blowing up along a singular line $y_2 = 0$ which in practice is not much more difficult than blowing up along a point.

Example 1.33. Now consider the curve of genus 2 that is given by the smooth projective model of the equation

$$y^2 = (x^2 + 1)(x^3 + p^6),$$

where $p = \pi$ is as above. The desingularization steps are essentially the same, and we shall keep the same notation.

The main difference is that now A is already a curve of genus 1, given by the equation

$$\pi' = 0, \quad y'^2 = x(x^2 + 1).$$

Hence $\mathcal{C}''$ is not only the minimal desingularization of $\mathcal{C}$, but also the minimal proper regular model of C over S, since A cannot be contracted if we want the model to remain regular. Obviously $\mathcal{C}$ does not have rational singularities.

At this point we can relate the Néron model $\mathcal{J}$ of the Jacobian of C to proper regular models. For this we now restrict to the case where R is a discrete valuation ring with valuation v. We first introduce a technical condition.

Definition 1.34. Let $\chi : \mathcal{C} \longrightarrow S$ be a proper regular model of C over S. Let $\Delta_1, \ldots, \Delta_n$ denote the geometric multiplicities of the irreducible components of the special fiber $\mathcal{C}_v$, see [9, §9, Definition 3]. We say that $\mathcal{C}$ *satisfies Condition* (†) if one of the following holds:

(a) The residue field is perfect and $\gcd(\Delta_1, \ldots, \Delta_n) = 1$.

(b) There is some i such that $\Delta_i = 1$.

Remark 1.35. Condition (†) is satisfied for any proper regular model of C over S if C has an l_v-rational point.

Whenever it is satisfied, this condition enables us to use Raynaud's results on Picard functors reproduced in [9, Chapter 9]. In the situations we are interested in, it will be obvious that Condition (†) is indeed satisfied – recall that from the beginning of the present thesis we have assumed that *any* residue field is perfect.

Let $\mathcal{C}$ be a proper regular model of C over S and let $\mathrm{Pic}_{\mathcal{C}/S}$ denote the relative Picard functor of $\mathcal{C}$ over S discussed in [9, Chapter 8]. We will have occasion to use the subfunctor $\mathrm{Pic}^0_{\mathcal{C}/S}$ of those elements of $\mathrm{Pic}_{\mathcal{C}/S}$ whose restriction to the special fiber $\mathcal{C}_v$ belongs to $\mathrm{Pic}^0_{\mathcal{C}_v/\mathfrak{l}}$ (cf. [9, §8.4]).

Theorem 1.36. *(Bosch, Lütkebohmert, Raynaud) Let $\mathcal{C}$ denote a proper model of C over S that satisfies Condition* (†)*. Then $\mathrm{Pic}^0_{\mathcal{C}/S}$ is representable as a separated scheme. Moreover, we have*

$$\mathcal{J}^0 \cong \mathrm{Pic}^0_{\mathcal{C}/S}\,.$$

if and only if $\mathcal{C}$ has rational singularities.

Proof. See [9, Theorem 9.5.4 (b)] (due to Raynaud) for the case of regular models. The statement there requires a condition that looks slightly different (involving the existence of an étale quasi-section) to hold, but [9, §9.5,

Remark 5] shows that it is equivalent to our Condition (†). The extension to rational singularities is [9, Theorem 9.7.1]. □

The final result of this section reduces the computation of the group of components Φ_v of $\mathcal{J}_v$ to an elementary group theory problem.

Proposition 1.37. *(Raynaud) Let $\mathcal{C}$ denote a proper regular model of C over S that satisfies Condition (†) and whose special fiber $\mathcal{C}_v$ over S has irreducible components $\Gamma_1, \ldots, \Gamma_n$ with respective multiplicities in $\mathcal{C}_v$ equal to $e_1, \ldots, e_n$. Let L denote the degree 0 part of the free abelian group on the components, that is*

$$L = \left\{ \sum_{i=1}^{n} a_i \Gamma_i : \sum_{i=1}^{n} a_i e_i = 0 \right\}.$$

Then Φ_v is isomorphic to the quotient of L by the subgroup of L generated by divisors of the form

$$\sum_{i=1}^{n} i_v(\Gamma_i, \Gamma_j)\Gamma_i,$$

where $j \in \{1, \ldots, n\}$.

Proof. See [9, Theorem 9.6.1]. The proof relies on Theorem 1.36 applied to regular models. □

1.6 Theta functions

Now we continue to look for interpretations of Néron functions. Having dealt with non-archimedean places, Néron constructs Néron functions for archimedean places v in [78]. The main idea is to use the complex uniformisation of abelian varieties over $\mathbb{C}$, so the construction does not distinguish between the cases $k_v = \mathbb{R}$ and $k_v = \mathbb{C}$. See [58], [75] or [49, §A.5] for foundational material concerning analytic abelian varieties.

Suppose A has dimension g. We view A as an abelian variety over the complex numbers embedded using v. Let $\mathfrak{h}_g$ denote the Siegel upper half space, that is the space of complex symmetric $g \times g$ matrices having positive definite imaginary part. There exists a unique element $\tau_v \in \mathfrak{h}_g$ such that $A(\mathbb{C})$ is isomorphic to $\mathbb{C}^g/\Lambda_v$, where $\Lambda_v = \mathbb{Z}^g \oplus \tau_v \mathbb{Z}^g$. We define a map j by

$$j : \mathbb{C}^g \twoheadrightarrow \mathbb{C}^g/\Lambda_v \xrightarrow{\cong} A(\mathbb{C}).$$

Definition 1.38. A *theta function with respect to* Λ_v is an entire function f on $\mathbb{C}^g$ such that

$$f(z+u) = \exp(g_u(z)) f(z) \text{ for all } z \in \mathbb{C}^g, u \in \Lambda_v,$$

where $g_u : \mathbb{C}^g \longrightarrow \mathbb{C}$ is a function satisfying

$$g_u(z + z') = g_u(z) + g_u(z') - g_u(0)$$

for all $z, z' \in \mathbb{C}^g$.

It turns out (see [58, Chapter X, Theorem 1.1]) that for each analytic divisor D of $A(\mathbb{C})$ (so in particular for any $D \in \mathrm{Div}(A)(\mathbb{C})$) we can find a theta function with respect to Λ_v having divisor $j^*(D)$. We say that two theta functions are *equivalent* if they have the same divisor.

In each equivalence class there is, up to multiplication by a nonzero constant, a unique theta function F that satisfies

$$F(z + u) = F(z) \exp\left(\pi H(z, u) + \frac{\pi}{2} H(u, u) + 2\pi i R(u)\right)$$

for all $z \in \mathbb{C}^g, u \in \Lambda_v$, where H is a Hermitian form (called the Hermitian form associated with F) and R is an $\mathbb{R}$-valued function. We call such a theta function a *normalized theta function*. See [58, Chapter 6] for facts concerning these functions. In particular we can associate a Hermitian form H_D to any divisor D and if D' is algebraically equivalent to D, then we have $H_{D'} = H_D$.

Proposition 1.39. *(Néron) Let $D \in \mathrm{Div}(A)(\mathbb{C})$ and let F_D be a normalized theta function with divisor $j^*(D)$ and associated Hermitian form H_D. Then the function*

$$\lambda_{D,v}(P) := -\log |F_D(z)|_v + \frac{\pi}{2} H_D(z, z)$$

on $A(\mathbb{C}) \setminus \mathrm{supp}(D)$ is a Néron function associated with D, where z is any element of $\mathbb{C}^g$ such that $j(z) = P$.

Proof. See [59, Chapter 13, Theorem 1.1]. □

This proposition will enable us to find Néron functions on Jacobians associated with the theta divisor and an archimedean place. Moreover, it will play an essential part in the determination of Green's functions in Chapter 5. In all these applications we are only concerned with certain types of theta functions. These we define now; they are of special interest on general complex abelian varieties for other reasons as well. For instance, one can always find a set of such functions that define a projective embedding of the abelian variety, see [75, §II.3]. We first define them on the product $\mathbb{C}^g \times \mathfrak{h}_g$.

Definition 1.40. Let $g \geq 1$ and $a, b \in \mathbb{Q}^g$. Let the function $\theta_{a,b}$ on $\mathbb{C}^g \times \mathfrak{h}_g$ be given by

$$\theta_{a,b}(z, \tau) = \sum_{m \in \mathbb{Z}^g} \exp\left(2\pi i \left(\frac{1}{2}(m + a)^T \tau (m + a) + (m + a)^T (z + b)\right)\right).$$

We call $\theta_{a,b}$ the *theta function with characteristic* $[a; b]$.

We fix an archimedean place v and an element $\tau = \tau_v$ of $\mathfrak{h}_g$ associated with our abelian variety and view theta functions as functions in one variable $z \in \mathbb{C}^g$. It is straightforward to check that such functions are indeed theta functions as defined above, cf. [75].

Remark 1.41. The function $\theta_{a,b}$ is not normalized. However, the function

$$\theta'_{a,b}(z) := \theta_{a,b}(z) \exp\left(\frac{\pi}{2} z^T (\operatorname{Im}\tau)^{-1} z\right)$$

is normalized and the associated Hermitian form is

$$H(z,w) := z^T (\operatorname{Im}\tau)^{-1} \bar{w},$$

where $\bar{w}$ is the complex conjugate of w. This can be verified using the transformation law of $\theta_{a,b}$ with respect to lattice points given, for instance, in [75, II, Theorem 6.6.1].

1.7 Applications

Since their introduction by Néron and Tate, canonical heights have found numerous applications. In this section we highlight a few, concentrating on those that require the actual *computation* of the canonical height. However, the canonical height also figures prominently in several important theorems in arithmetic geometry, including Faltings' Theorem, stating that a curve of genus greater than one defined over a number field has only finitely many rational points (especially in the proof that uses Vojta's inequality which is phrased in terms of the canonical height with respect to the theta divisor on its Jacobian, see [49, Chapter E]).

Furthermore, the canonical height substantially simplifies the proof of the Mordell-Weil Theorem for abelian varieties, more precisely the step that the so-called "weak" Mordell-Weil Theorem implies the full Mordell-Weil Theorem (see [49, Chapter C]).

Suppose that $A = J$ is the Jacobian of a smooth projective curve C of positive genus g defined over a number field k. In many cases one is interested in actually determining a set of generators for the Mordell-Weil group $J(k)$.

This is an interesting problem in its own right, but also useful for other purposes as well. If, for instance, $k = \mathbb{Q}$, then a method for the computation of the $\mathbb{Z}$-rational points on a hyperelliptic curve itself is discussed in [14]. This approach uses linear forms in logarithms and the Mordell-Weil sieve described in [13], but requires, in addition, a set of generators for the full Mordell-Weil group.

So suppose that we have already computed the rank r of $J(k)$. If the dimension of J is small, then in many cases this can be done using 2-descent

(see [93] for an implementation-oriented description); more generally one uses n-descent for $n \geq 2$ or descent by isogeny (see [85] for a general conceptual framework). Even if one cannot calculate the rank exactly using these approaches, it is often possible to give an upper bound. There are methods to search for k-rational points on the Jacobian, for example Stoll's program `j-points` [96] for the genus 2 case if $k = \mathbb{Q}$. Suppose we have found r points $P_1, \ldots, P_r \in J(k)$ that are independent (see below). Then we know that $H = \langle P_1, \ldots, P_r \rangle$ is a subgroup of $J(k)$ of finite index. It turns out that in order to saturate this subgroup, it suffices to have

(a) a method to compute the canonical height $\hat{h}_D$ with respect to an ample symmetric divisor class $[D]$ on J,

(b) a method to list all points in $J(k)$ with height $\hat{h}_D$ bounded by a constant B.

Step (b) can be split up into two steps if we can

(b') list all points in $J(k)$ with height h_D bounded by a given constant B, where h_D is some choice of Weil height function on J with respect to D,

(b") bound the difference $\hat{h}_D - h_D$.

An algorithm that uses (a), (b') and (b") to compute generators of the Mordell-Weil group from the knowledge of r and an independent set of r points $P_1, \ldots, P_r$ is presented in [94, §7]. In this thesis we are mostly concerned with (a), although we shall discuss (b") occasionally. Step (b') is possible using `j-points` in the genus 2 case.

Using part (iii) of Theorem 1.3 it is easy to decide for any abelian variety A/k whether a given point $P \in A(\bar{k})$ has finite order. How can we decide whether elements of the Mordell-Weil group are independent?

Definition 1.42. Let k be a number field and A/k an abelian variety defined over k. Let $D \in \mathrm{Div}(A)(k)$ such that $[D] \in \mathrm{Pic}(A)$ is ample and symmetric and let $\hat{h}_D$ be the canonical height on A with respect to D.

(i) The *canonical height pairing* or *Néron-Tate pairing on A with respect to D* is the bilinear pairing

$$\begin{aligned} (\cdot,\cdot)_D : A(\bar{k}) \times A(\bar{k}) &\longrightarrow \mathbb{R} \\ (P, Q) &\mapsto \frac{\hat{h}_D(P+Q) - \hat{h}_D(P) - \hat{h}_D(Q)}{2}. \end{aligned}$$

(ii) Let $P_1, \ldots, P_n \in A(\bar{k})$. The *regulator of $P_1, \ldots, P_n$ with respect to D* is the quantity

$$\mathrm{Reg}_D(P_1, \ldots, P_n) := \det\left(((P_i, P_j)_D)_{1 \leq i,j \leq n}\right).$$

(iii) The *regulator of $A(k)$ with respect to D* is the regulator of $P_1, \dots, P_r$, where $P_1, \dots, P_r$ is any independent set of generators of the free part of $A(k)$. We denote it by $\mathrm{Reg}_D(A/k)$.

From Theorem 1.3 we see that the canonical height pairing is a positive definite quadratic form on $A(\bar{k})/A(\bar{k})_{\mathrm{tors}}$ and that the regulator of any set of points in $A(\bar{k})$ is nonnegative. Therefore, the regulator of a set of points vanishes if and only if that set is dependent, leading to an effective method to check independence.

The regulator of an abelian variety also appears in the formulation of the Birch and Swinnerton-Dyer conjecture. We only introduce the conjecture over $\mathbb{Q}$, but it can be formulated over general number fields; furthermore we introduce most terms without explaining them, see [49, §F.4.1] for a more elaborate (but still concise) discussion.

Instead of allowing the regulator with respect to arbitrary ample symmetric divisors which would introduce some ambiguity, one looks at the so-called *canonical regulator*, that is the regulator with respect to the Poincaré divisor on the product $A \times \hat{A}$, where $\hat{A}$ is the dual abelian variety to A. The relation between this quantity and the regulator with respect to a fixed ample symmetric divisor on A is explained in [49, Remark F.4.1.3], but we are not concerned with this difficulty, as Jacobians are self-dual. Let $L(A, s)$ denote the L-series of A whose convergence for $\mathrm{Re}(s) > 3/2$ follows by definition, Ω_A the real period of a certain differential, called the Néron differential by Hindry and Silverman, c_p the Tamagawa number $\#\Phi_p(\mathbb{F}_p)$ for any $p \in M_{\mathbb{Q}}^0$ and $Ш(A/\mathbb{Q})$ the Shafarevich-Tate group.

Conjecture 1.43. *(Birch and Swinnerton-Dyer)*

(i) *$L(A, s)$ has a zero at $s = 1$ of order equal to the rank r of $A(\mathbb{Q})$.*

(ii) *The Taylor expansion of $L(A/\mathbb{Q}, s)$ around $s = 1$ has leading coefficient*

$$\lim_{s \to 1} \frac{L(A, s)}{(s-1)^r} = \Omega_A \left(\prod_{p \in M_{\mathbb{Q}}^0} c_p \right) \frac{\#Ш(A/\mathbb{Q}) \,\mathrm{Reg}(A/\mathbb{Q})}{\#A(\mathbb{Q})_{\mathrm{tors}} \#\hat{A}(\mathbb{Q})_{\mathrm{tors}}}.$$

In order for the conjecture to make sense, we need to assume that $L(A, s)$ has a suitable analytic continuation; in fact it is conjectured to have an analytic continuation to all of $\mathbb{C}$. Moreover, finiteness of Ш is conjectured, but not known. However, under the assumption that Ш is indeed finite, its order must be a nonnegative integer, so if we can compute the other terms, some of which are transcendental, we can gather experimental evidence for the conjecture. This has been done for specific elliptic curves by several authors, starting with Birch and Swinnerton-Dyer in [5] - in fact the numerical results led them to the formulation of the conjecture, which was originally phrased

for elliptic curves and only later extended by Tate to general abelian varieties in [101]. Other examples include [15] and [27], see also the recent thesis of Miller [71], where the conjecture is verified for all elliptic curves of small conductor except for a few exceptions.

For abelian varieties of higher dimension much less has been done. The only two examples that the author is aware of are the work by Yoshida [104] dealing with a specific modular Jacobian of dimension 2 and another paper [44] by Flynn et al. where they undertake a more systematic study of a number of modular Jacobians of dimension 2. Here "modular" means that the Jacobian is a quotient of the Jacobian of a modular curve $X_0(N)$ for some level N; it is natural to first consider such Jacobians because the analytic continuation of L-series associated to modular forms – and hence the analytic continuation of $L(A, s)$ – is known.

Notice that the ability to compute canonical heights explicitly comes in twice if we wish to collect evidence for the Birch and Swinnerton-Dyer conjecture: We need it to find a basis for the Mordell-Weil group of A and we need it - and this basis - to compute the regulator. Since up to now no method has been found to compute canonical heights for Jacobians of curves of genus at least 3, it has not been possible to check the plausibility of the conjecture in such cases (unless the Mordell-Weil rank vanishes). We develop a method for the computation of canonical heights on arbitrary Jacobians in Chapter 5.

Chapter 2

Elliptic curves

2.1 Heights on elliptic curves

Let l be a field. We consider elliptic curves given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in l, \tag{2.1}$$

where the discriminant Δ of the equation is nonzero.

For now E denotes an elliptic curve given by a Weierstrass equation (2.1) over a number field or one-dimensional function field k with algebraic closure $\bar{k}$. Without loss of generality we may assume that $a_i \in \mathcal{O}_k$ for all i, so that the given Weierstrass equation is an $\mathcal{O}_k$-integral model of E in the sense of Definition 1.12.

In order to develop a reasonable height theory on E it is necessary to pick an ample symmetric k-rational divisor class on E. A natural choice is a multiple of the class of the divisor (O), where O is the identity of the group law on E. We choose the class of $D = 2(O)$ and retain this notation for the remainder of this chapter. The linear system associated to this divisor is base point free and a map to projective space corresponding to a basis of $\mathcal{L}(2(O))$ is given by

$$\begin{array}{rccc} \kappa: & E & \longrightarrow & \mathbb{P}^1 \\ & (x,y) & \mapsto & (x:1) \\ & O & \mapsto & (1:0). \end{array}$$

Definition 2.1. Let E/k be an elliptic curve defined by an $\mathcal{O}_k$-integral Weierstrass equation (2.1). The function $h : E(\bar{k}) \longrightarrow \mathbb{R}$ given by

$$h(P) := h_D(P) := \frac{1}{d_k} \sum_{v \in M_k} -N_v \min\{v(x(P)), 0\}$$

is called the *naive height on* E. The *canonical height on* E is the function

$$\begin{array}{rccc} \hat{h} : E(\bar{k}) & \longrightarrow & \mathbb{R} \\ P & \mapsto & \lim\limits_{n\to\infty} \frac{1}{4^n} h\left(2^n P\right). \end{array}$$

Note that this is in accordance with our constructions from Section 1.2.

2.2 Local heights

We now decompose the canonical height into a sum of canonical local heights using Theorem 1.8. Let k_v be the completion of a number field or one-dimensional function field k and consider an elliptic curve E defined over k_v and given by an equation of the form (2.1), where we may assume that the coefficients a_i lie in the ring of integers $\mathcal{O}_v$ of k_v.

Consider the functions ψ_2 and ϕ_2 defined in [86, Exercise III.7] as

$$\begin{aligned}\psi_2(P) &:= 4x(P)^3 + b_2x(P)^2 + 2b_4x(P) + b_6,\\ \phi_2(P) &:= x(P)^4 - b_4x(P)^2 - 2b_6x(P) - b_8,\end{aligned}$$

where the b_i are the usual well-known polynomials in the a_i, see [86, §3.2]. If $P, 2P \neq O$ we have $x(2P) = \phi_2(P)/\psi_2(P)$ (see loc. cit.). We find

$$[2]^*(D) = 4D + \operatorname{div}(\psi_2).$$

This is because the normalization $(x(P), 1)$ of $\kappa(P)$ for $P \neq O$ corresponds to the choice of the divisor D in its class $[D]$. In order to use Theorem 1.8 we set

$$\lambda_v(P) := -\frac{N_v}{n_v}\min\{v(x(P)), 0\} = \max\{\log|x(P)|_v, 0\}$$

for $P \in E(k_v)\backslash\{O\}$. It is easy to see that λ_v is a Weil function on $E(k_v)\backslash\{O\}$. If $P, 2P \neq O$, then we get

$$\lambda_v(2P) - 4\lambda_v(P) = -\log|\psi_2(P)|_v - \frac{N_v}{n_v}\varepsilon_v(P),$$

where

$$\varepsilon_v(P) = \min\{v(\psi_2(P)), v(\phi_2(P))\} - 4\min\{0, v(x(P))\}$$

is bounded and continuous in the v-adic topology.

According to Proposition 1.6, we can now define canonical local heights on elliptic curves.

Definition 2.2. Let E/k_v be an elliptic curve defined over the completion k_v of a number field or a one-dimensional function field k at a place $v \in M_k$. The function $\hat{\lambda}_v : E(k_v) \setminus \{O\} \longrightarrow \mathbb{R}$ defined by

$$\hat{\lambda}_v(P) := -\frac{N_v}{n_v}(\min\{v(x(P)), 0\} - \mu_v(P))$$

is called the *canonical local height on E,* where

$$\mu_v(P) = \sum_{n=0}^{\infty}\frac{1}{4^{n+1}}\varepsilon_v(2^nP).$$

So the canonical local height at v is the canonical local height associated with $2(O), v$ and ψ_2.

Now suppose that E is defined over k. Then we have

$$h(P) = \frac{1}{d_k}\sum_{v\in M_k} n_v\lambda_v(P)$$

and from Theorem 1.8 we deduce

$$\hat{h}(P) = \frac{1}{d_k}\sum_{v\in M_k} n_v\hat{\lambda}_v(P).$$

for all $P \in E(k) \setminus \{O\}$.

Remark 2.3. There are several normalizations in use for the canonical height and even more for the canonical local height on elliptic curves. Our normalization $\hat{\lambda}_v$ of the canonical local height on elliptic curves defined below corresponds to the one used in [28], so in particular we have

$$\hat{\lambda}_v(P) = 2\hat{\lambda}_v^{\mathrm{SilB}}(P) - \frac{1}{6}v(\Delta) \tag{2.2}$$

where $\hat{\lambda}_v^{\mathrm{SilB}}$ is the normalization used in Silverman's second book [89, Chapter VI] on elliptic curves and Δ is the discriminant of the given Weierstrass model of E. The advantages of this normalization are discussed in [28]; the most important property that $\hat{\lambda}_v^{\mathrm{SilB}}$ satisfies is independence of the model. This follows from Proposition 2.5 below.

The key properties that the canonical local height, normalized as above, satisfies are summarized in the following theorem.

Theorem 2.4. *(Néron, Tate) Let E be an elliptic curve defined over k_v. Then the canonical local height $\hat{\lambda}_v$ on E satisfies the following properties:*

(i) *$\hat{\lambda}_v$ is continuous on $E(k_v) \setminus \{O\}$ and bounded on the complement of any open neighborhood of O with respect to the v-adic topology.*

(ii) *The v-adic limit*
$$\lim_{P \to O}(\hat{\lambda}_v(P) - \log|x(P)|_v)$$
exists.

(iii) *For all $P \in E(k_v) \setminus \{O\}$ with $2P \neq O$ we have*
$$\hat{\lambda}_v(2P) - 4\hat{\lambda}_v(P) = \log|\psi_2(P)|_v$$

(iv) *For all $P, Q \in E(k_v) \setminus \{O\}$ such that $P \pm Q \neq O$ we have*
$$\hat{\lambda}_v(P+Q) + \hat{\lambda}_v(P-Q) = 2\hat{\lambda}_v(P) + 2\hat{\lambda}_v(Q) - 2\log|x(P) - x(Q)|_v.$$

(v) *If k'/k_v is a finite extension and v' is the extension of v to k', then we have $\hat{\lambda}_{v'}(P) = \hat{\lambda}_v(P)$ for all $P \in E(k_v)$.*

Moreover, $\hat{\lambda}_v$ is determined uniquely by $(i) - (iii)$.

Proof. For a proof of results corresponding to (i)-(iii) and (v) for $\hat{\lambda}_v^{\mathrm{SilvB}}$ see [89, Chapter VI, Theorem 1.1]. Part (iv) for $\hat{\lambda}_v^{\mathrm{SilvB}}$ is proved as [89, Chapter VI, Corollary 3.3] for archimedean v and is [89, Exercise 6.3] for non-archimedean v; the properties of $\hat{\lambda}_v^{\mathrm{SilB}}$ proved in [89] translate easily to our situation using (2.2). In fact part (iii) and (assuming the other properties have been verified) uniqueness are immediate from Proposition 1.6, parts (i) and (ii). □

For several applications it is important to know how the canonical local height changes under isogenies.

Proposition 2.5. *(Bernardi) Let E and E' be elliptic curves defined over k_v and given by Weierstrass models with respective discriminants Δ and Δ'. Let $\alpha : E \longrightarrow E'$ be an isogeny of degree d and let $\hat{\lambda}_v$ denote the canonical local height, see Definition 2.2. If $P \in E(k_v)$ satisfies $\alpha(P) \neq 0$, then we have*

$$\hat{\lambda}_v(\alpha(P)) = d\hat{\lambda}_v(P) + v(F_\alpha(P)) + \frac{1}{6}v(m(\alpha)),$$

where

$$F_\alpha(P) = \prod_{Q \in \ker(\alpha)\setminus\{O\}} (x(P) - x(Q))$$

and

$$m(\alpha) = \lim_{P \to O} \left(\frac{x(P)}{x(\alpha(P))} \right)^6 \frac{\Delta'}{\Delta}.$$

Proof. See [4]. □

Remark 2.6. We can use Proposition 2.5 to find out how the canonical local height behaves under changes of the model. Another application is discussed in Section 2.4.

We want to stress that the normalization of the canonical local height introduced in Definition 2.2 very much depends on the normalization $\kappa(P) = (x(P), 1)$ corresponding to the choice of $D = 2(O)$ in its linear equivalence class. We could instead define the canonical local height not on the elliptic curve itself, but on the image $\kappa(E) = \mathbb{P}^1$, or even on

$$K_{\mathbb{A}} := \{(x_1, x_2) \in \mathbb{A}^2 : \exists P \in E \text{ such that } \kappa(P) = (x_1 : x_2)\} = \mathbb{A}^2 \setminus \{(0,0)\}$$

as follows: The polynomials ψ_2 and ϕ_2 only depend on the x-coordinate of P. We can extend the relation $x(2P) = \phi_2(x(P))/\psi_2(x(P))$ to all of E by letting $F(X, Z)$ and $G(X, Z)$ be the degree 4 homogenizations of ψ_2 and ϕ_2, respectively. Hence we have

$$\kappa(2P) = (G(\kappa(P)) : F(\kappa(P))).$$

It is easy to see that with these definitions $\varepsilon_v(P)$ does in fact not depend on the normalization $(x(P), 1)$ for $(\kappa_1(P) : \kappa_2(P)))$. Let

$$\delta(x_1, x_2) := (F(x_1, x_2), G(x_1, x_2)).$$

Then we have $\delta(1, 0) = (1, 0)$ and if $x = (x_1, x_2) \in K_{\mathbb{A}}$ represents $\kappa(P)$ for some $P \in E$, then we know that $\delta(x)$ represents $\kappa(2P)$.

Definition 2.7. Suppose $x = (x_1, x_2) \in K_{\mathbb{A}}(k_v)$. Then we define

$$\varepsilon_v(x) := \min\{v(\delta_1(x)), v(\delta_2(x))\} - 4\min\{v(x_1), v(x_2)\}$$

and

$$\mu_v(x) := \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \varepsilon_v(\delta^{\circ n}(x)).$$

It follows that we have $\varepsilon_v(P) = \varepsilon_v(x)$ and $\mu_v(P) = \mu_v(x)$ whenever x represents $\kappa(P)$ for some $P \in E(k_v)$. Hence it makes sense to define a canonical local height on $K_{\mathbb{A}}(k_v)$ as follows:

Definition 2.8. The *canonical local height on* $K_{\mathbb{A}}(k_v)$ is the function mapping $x = (x_1, x_2) \in K_{\mathbb{A}}(k_v)$ to

$$\hat{\lambda}_v(x) := -\frac{N_v}{n_v} \left(\min\{v(x_1), v(x_2)\} - \mu_v(x)\right).$$

Suppose that E is defined over k and $P \in E(k)$. Because of the product formula (1.1) the normalization of $\kappa(P)$ that is encoded in the expression $\min\{v(x_1), v(x_2)\}$ does not contribute globally if we sum up all over all places $v \in M_k$, so we have

$$\hat{h}(P) = \frac{1}{d_k} \sum_{v \in M_k} n_v \hat{\lambda}_v(x)$$

for any $x \in K_{\mathbb{A}}(k)$ representing $\kappa(P)$. This construction has the advantage that it does not depend on the choice of a divisor in its divisor class and is therefore defined for any point on the curve. Furthermore, the properties that this canonical local height enjoys are better in some sense; for example, the identities

$$\hat{\lambda}_v(\delta(x)) = 4\hat{\lambda}_v(x)$$

and

$$\hat{\lambda}_v(x) = \lim_{n \to \infty} 4^{-n} \hat{\lambda}_v(\delta^{\circ n}(x))$$

follow immediately from the definitions.

We will generalize this construction to the case of Jacobian surfaces later on.

2.3 Non-archimedean places

We constructed canonical local heights on an elliptic curve E defined over k_v in the previous section. Now we want to discuss how we can explicitly compute the values of these functions in practice, first for non-archimedean v. We start with the following definition.

Definition 2.9. Let C/l be a smooth projective curve defined by an R-integral model over the fraction field l of a discrete valuation ring R whose closure $\mathcal{C}$ over $S = \mathrm{Spec}(R)$ is normal and flat. We say that the model of C is *geometrically minimal* if the minimal desingularization of $\mathcal{C}$ is isomorphic to the minimal proper regular model of C over S.

Example 2.10. If $p > 3$ is a prime number, then the closure of the Weierstrass model

$$y^2 = x^3 + p^6$$

over $\mathrm{Spec}(\mathbb{Z}_p)$ is not geometrically minimal (see Example 1.32 and Lemma 2.12), but the closure of the model

$$y^2 = (x^2 + 1)(x^3 + p^6)$$

over $\mathrm{Spec}(\mathbb{Z}_p)$ is geometrically minimal (see Example 1.33 and Remark 3.31).

Remark 2.11. As in the examples, geometric minimality is usually not hard to check in practice, assuming we can compute desingularizations and contractions. It is equivalent to the statement that the minimal proper regular model is a desingularization of the closure over R of the model of C.

This condition was discovered to be of interest by Sadek, see [84]. We use his terminology.

We first prove a lemma that characterizes v-minimal Weierstrass models in geometric terms. Recall that we are interested in elliptic curves defined over k_v, where v is non-archimedean.

Lemma 2.12. *Let E/k_v be an elliptic curve given by an $\mathcal{O}_v$-integral Weierstrass equation. The given model is geometrically minimal if and only if it is v-minimal.*

Proof. This can be verified in a very computational manner. It is clear that the closure $\mathcal{C}$ over $\mathrm{Spec}(\mathcal{O}_v)$ of the given equation is normal and flat and so it is a model of E over $\mathrm{Spec}(\mathcal{O}_v)$. We can use Tate's algorithm for the computation of the minimal proper regular model discussed in [89, §IV.9] and note that if the model we start with is v-minimal, we never get to the final step of the algorithm. Because no contractions occur, this process yields a desingularization of $\mathcal{C}$.

If, on the other hand, the model is not v-minimal, then the special fiber at the last step of the algorithm consists of three components A, D and B, where A has mutliplicity 1 and is the strict transform of the nonsingular part of $\mathcal{C}_v$, D has multiplicity 2 and B has multiplicity 1 (see Example 1.32). However, the transformation acting on an affine point (ξ, η) by $(\xi, \eta) \mapsto (\pi^{-2}\xi, \pi^{-3}\eta)$ which is applied at this point corresponds to contracting D and B and restarting the algorithm with a Weierstrass equation whose reduction modulo π is B instead of $\mathcal{C}_v$. Hence the minimal proper regular model cannot be a desingularization of $\mathcal{C}$. □

This result is also proved by Conrad in [24, Corollary 4.7], by Liu in [65, §9.4] and by Sadek in [84, Theorem 4.1]. Note that these proofs do not use Tate's algorithm at all; indeed, Sadek's proof generalizes to models of genus one curves of degree ≤ 4 that have a k_v-rational point. Geometric minimality provides a non-explicit and hence sometimes more convenient way of identifying v-minimality, as explained in [84].

In addition, Conrad proves the following result that will come up again in Chapter 3:

Lemma 2.13. *The closure of an $\mathcal{O}_v$-integral Weierstrass model of an elliptic curve has rational singularities if and only if the model is v-minimal.*

Proof. Instead we can check directly using Remark 1.27 that closures of v-minimal Weierstrass models have rational singularities by computing the possible fundamental cycles and using the adjunction formula to find its arithmetic genus. Conversely, it is easy to see that if the model is not v-minimal, then a desingularization of its closure necessarily includes at least one normalization step as in Example 1.32. See [24, Corollary 8.4] for a more conceptual proof. □

In Section 1.4 we have related the computation of Néron functions to the Néron model $\mathcal{E}$ of E over the spectrum of the ring of integers $\mathcal{O}_v$ of the completion k_v. We let π denote a uniformiser and $\mathfrak{k}_v$ the residue field of $\mathcal{O}_v$. It is verified in [89, Chapter IV, Theorem 6.1] that for elliptic curves the Néron model at v can be constructed by discarding all singular points from the special fiber of the minimal proper regular model $\mathcal{C}^{\min}$ of E over $\operatorname{Spec}(\mathcal{O}_v)$ defined in Theorem 1.28.

Proposition 2.14. *Let E/k_v be an elliptic curve given by an $\mathcal{O}_v$-integral Weierstrass equation that is v-minimal.*

(i) *The values of ε_v and μ_v at $P \in E(k_v)$ only depend on the component of the special fiber $\mathcal{E}_v$ that P maps to.*

(ii) *We have $\varepsilon_v(P) = \mu_v(P) = 0$ for $P \in E(k_v)$ mapping to the identity component.*

Proof. By virtue of Lemma 2.12 we only need blow-ups in order to form the minimal proper regular model from the closure $\mathcal{C}$ over $\operatorname{Spec}(\mathcal{O}_v)$ of the given model. Recall that according to Theorem 1.17 there are constants $\gamma_j(D) = \gamma_j(2(O))$ for each of the components $\mathcal{E}_v^j \in \{\mathcal{E}_v^0, \ldots, \mathcal{E}_v^n\}$, where $\mathcal{E}_v^0$ is the identity component, such that for all $P \in E(k_v) \setminus \{O\}$ mapping to $\mathcal{E}_v^j$ we have

$$\hat{\lambda}_v(P) = \frac{N_v}{n_v}(i(D,P) + \gamma_j(D)),$$

where $i(D,P)$ was defined in (1.3).

The Néron model is simply the smooth part of the minimal proper regular model. Hence it follows from (1.4) that in the case of an elliptic curve $i(D,P)$ coincides with the usual intersection multiplicity $i_v(D_{\mathcal{C}^{\min}},(P)_{\mathcal{C}^{\min}})$, introduced in Definition 1.29, on the minimal proper regular model $\mathcal{C}^{\min}$ over $\mathrm{Spec}(\mathcal{O}_v)$. Moreover, a blow-up is an isomorphism outside of its center (see the beginning of Section 5.3.4). Therefore Lemma 2.12 guarantees that if P reduces to a regular point modulo v, then we can compute $i(D,P)$ as the intersection multiplicity of the Zariski closures $D_{\mathcal{C}}$ and $(P)_{\mathcal{C}}$ over $\mathcal{C}$.

In other words, we have

$$i(D,P) = -\min\{v(x(P)),0\}$$

and therefore

$$\mu_v(P) = \frac{n_v}{N_v}\hat{\lambda}_v(P) - \min\{v(x(P)),0\} = -\gamma_0(D),$$

for points mapping to the identity component proving part (i) for such points. If, on the other hand, a point satisfies $v(x(P)) \geq 0$, then the points P and O do not reduce to the same point modulo v, so Lemma 2.12 implies that $i(D,P)$ vanishes for any point mapping to a non-identity component $\mathcal{E}_v^j$.

This shows that

$$\mu_v(P) = -\frac{n_v}{N_v}\hat{\lambda}_v(P) = -\gamma_j(D)$$

only depends on j and also implies the same assertion for ε_v, because of

$$\varepsilon_v(P) = 4\mu_v(P) - \mu_v(2P).$$

In order to prove part (ii) it is enough to show that $\varepsilon_v(P)$ vanishes for any $P \in E(k_v)$ mapping to $\mathcal{E}_v^0$; this is done in the proof of [89, Chapter IV, Theorem 4.1] and we do not repeat it here. □

Remark 2.15. We slightly abuse notation by saying that ε_v and μ_v factor through the component group Φ_v whenever (i) and (ii) are satisfied. See the discussion of Φ_v in Section 1.4.

Remark 2.16. A simple formula expressing $\gamma_j(D)$ and hence $\hat{\lambda}_v$ in terms of intersection multiplicities is proved in [18]; see also [28] where all possible values of the $\gamma_j(D)$ are determined in order to give optimal bounds for the difference between the naive local height and the canonical local height in the non-archimedean situation (see Section 1.7).

Suppose from now on that the given Weierstrass model of E is v-minimal. Given any Weierstrass equation we can find such a v-minimal equation using Tate's algorithm or using a much faster algorithm due to Laska [61]. The component groups of Néron models of elliptic curves are well-understood

and can be computed using Tate's algorithm. If, for instance, the curve has multiplicative reduction and $m = v(\Delta)$ (Kodaira type I_m), then over the algebraic closure of $\mathfrak{k}_v$ the special fiber of $\mathcal{C}^{\min}$ is an m-gon and we have

$$\Phi_v \cong \mathbb{Z}/m\mathbb{Z}.$$

In all other cases we have

$$\Phi_v \cong G, \text{ where } G \in \{\{0\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\}$$

(see [89, §IV.8]).

In order to find formulas for $\hat{\lambda}_v$ we use Proposition 2.14. We need the polynomial ψ_2 introduced above, as well as the triplication polynomial ψ_3 (see [87]) satisfying

$$\hat{\lambda}_v(3P) = 9\hat{\lambda}_v(P) - \log|\psi_3(P)|_v.$$

Algorithm 1 Computation of $\hat{\lambda}_v(P)$

if P maps to $\mathcal{E}_v^0$ **then**
  return $-\frac{N_v}{n_v}\min\{v(x(P)), 0\}$
else if $v(c_4(E)) = 0$ **then**
  $m \leftarrow v(\Delta)$
  $n \leftarrow \min\{v(2y(P) + a_1x(P) + a_3), m/2\}$
  return $-\frac{N_v}{n_v}\frac{n(m-n)}{m}$
else if $v(\psi_3(P)) \geq v(\psi_2(P))$ **then**
  return $-\frac{2N_v}{3n_v}v(\psi_2(P))$
else
  return $-\frac{N_v}{4n_v}v(\psi_3(P))$
end if

Theorem 2.17. *(Néron, Tate, Silverman) Suppose $P \in E(k_v)$. Then Algorithm 1 returns the canonical local height $\hat{\lambda}_v(P)$.*

Proof. See [87, Theorem 5.2]. The history of the results is briefly discussed following [28, Proposition 5]. Note that if E has bad reduction, then the condition $v(c_4(E)) = 0$ is satisfied precisely when E has multiplicative reduction (see [86, Proposition 5.1]). Here $c_4(E)$ is a well-known invariant of E defined in [86, §III.1]. □

Due to Silverman's work in [87] all steps can be made both effective and efficient.

2.4 Archimedean places

Let v be an archimedean place of a number field k. Then we either have $k_v = \mathbb{R}$ or $k_v = \mathbb{C}$. Several methods have been proposed for the computation of the canonical local height $\hat{\lambda}_v$. We first discuss an approach due to Tate with modifications by Silverman, then a completely different method due to Néron and Silverman and finally an algorithm devised by Bost and Mestre.

Tate's approach seems to be quite natural from our setup because it uses Definition 2.2. Namely, we compute N terms of the infinite converging series defining $\mu_v(P)$, where N is chosen to guarantee the desired accuracy. This integer can be found by observing that the error we have if we cut off the series after N terms is of order 4^{-N}. Therefore the series converges linearly. The exact error is given in [87, Theorem 4.2].

Tate's original series is only guaranteed to converge in all cases if $k_v = \mathbb{R}$, but this was fixed by Silverman in [87]. The idea is to switch to a slightly different series whenever the terms become too large. A similar method for guaranteeing convergence would be to use our canonical local heights for pairs $x = (x_1, x_2) \in K_{\mathbb{A}}$. This construction allows us to renormalize the pairs at each step, so that convergence can be ensured easily.

Although Tate presented the first practical method for the computation of $\hat{\lambda}_v$, there are more efficient methods available now in case v is real.

One algorithm depends on the original construction of Néron functions for archimedean places due to Néron and discussed in Proposition 1.39. Suppose E is embedded into $\mathbb{P}^2_{\mathbb{C}}$ using v and recall the notation from Section 1.6. Let $\tau_v \in \mathbb{H} = \mathfrak{h}_1$ such that $E(\mathbb{C})$ is isomorphic to $\mathbb{C}/\Lambda_v$, where $\Lambda_v = \mathbb{Z} \oplus \tau_v\mathbb{Z}$ and let j be the composition

$$j : \mathbb{C} \twoheadrightarrow \mathbb{C}/\Lambda_v \xrightarrow{\cong} E(\mathbb{C}).$$

Moreover, let $\sigma(z) = \sigma(z, \Lambda_v) : \mathbb{C} \longrightarrow \mathbb{C}$ be the Weierstrass σ-function, $\eta : \mathbb{C} \cong \Lambda_v \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow \mathbb{C}$ the extension of the quasi-period map to an $\mathbb{R}$-linear homomorphism, see [89, Chapter I]. Let $q = \exp(2\pi i \tau_v)$ and recall the Definition 2.2 of the canonical local height.

Proposition 2.18. *(Néron) The canonical local height is given by*

$$\begin{aligned} \hat{\lambda}_v(P) &= -\log \left| \exp(-\frac{1}{2} z\eta(z))\sigma(z) \right|_v \\ &= -\log \left| q^{\frac{w^2-w}{2}}(1-u) \prod_{n\geq 1} \frac{(1-q^n u)(1-q^n u^{-1})}{(1-q^n)^2} \right|_v , \end{aligned}$$

where $P \in E(\mathbb{C}) \setminus \{O\}$, $z \in \mathbb{C}$ is any complex number satisfying $j(z) = P, u = \exp(2\pi i z)$ and $w = \frac{\operatorname{Im} z}{\operatorname{Im} \tau_v}$.

Proof. See [89, Chapter VI, Theorems 3.2, 3.4]. □

Remark 2.19. Proposition 2.18 provides the simplest example for Proposition 1.39.

The question is how this result can be used for practical purposes. The fact that we can compute the canonical local height using Proposition 2.18 relies on three computational "tricks"; however, they only work for real embeddings. So suppose v is real. First, it is possible to compute τ_v using the quadratically converging arithmetic-geometric mean. This is basically due to Gauss and is described by Bost and Mestre in [11]; see also [23, Algorithm 7.4.7]. Second, a very similar method can be used to compute the elliptic logarithm of a point $P \in E(\mathbb{C})$, that is an element $z \in \mathbb{C}$ satisfying $j(z) = P$ and an additional normalization condition. This technique is sometimes called Landen's transformation, cf. [11] and [23, Algorithm 7.4.8]. Finally, the σ-function can be computed in practice in terms of the sine-function using a trick due to Silverman. The complete algorithm can be found in [23, Algorithm 7.5.7]. This method can be shown to be indeed faster than Tate's series, especially if one is interested in high precision of the result.

The third method available for the computation of the canonical local height on an elliptic curve at an archimedean place is due to Bost and Mestre. The purpose of the remainder of this section is merely to give a summary of the unpublished manuscript [12]; to the author's knowledge the only additional reference is an implementation in `Pari` [79]. The algorithm uses the arithmetic-geometric mean and goes as follows: We first use an isogeny to make sure that our elliptic curve is embedded in $\mathbb{P}^2_{\mathbb{R}}$ using v and given by a simplified Weierstrass model

$$E_0 : y^2 = x(x + a_0^2)(x + b_0^2),$$

where $a_0, b_0 \in \mathbb{R}_{\geq 0}$. For $n \geq 1$ we recursively define an elliptic curve over the real numbers by

$$E_n : y^2 = x(x + a_n^2)(x + b_n^2),$$

where

$$a_n = \frac{a_{n-1} + b_{n-1}}{2}, b_n = \sqrt{a_{n-1} b_{n-1}}$$

and we define the 2-isogeny $\phi_{n-1} : E_n \to E_{n-1}$ by

$$(x, y) \mapsto \left(\frac{x(x + b_n^2)}{x + a_n^2}, y \frac{(x + a_{n-1} a_n)(x + b_{n-1} a_n)}{(x + a_n^2)^2} \right).$$

Now let $\hat{\lambda}_n$ denote the canonical local height on $E_n(\mathbb{R})$. Then Proposition 2.5 asserts

$$\hat{\lambda}_{n-1}(P_{n-1}) = 2\hat{\lambda}_n(P_n) - \log |x(P_n) + a_n^2|, \tag{2.3}$$

whenever we have $P_{n-1} = \phi_{n-1}(P_n)$ and $x(P_{n-1}) \neq 0$. We want to give a recursive formula for the canonical local height, so we restrict ourselves to affine points $P_0 = (x_0, y_0) \in E_0(\mathbb{R})$ lying on the connected component of the identity of $E_0(\mathbb{R})$, since such points always have a preimage in $E_1(\mathbb{R})$ under ϕ_0 and moreover this preimage is guaranteed to lie on the connected component of the identity of $E_1(\mathbb{R})$. In general $2P$ lies in this component for any point P and we can use part (iii) of Theorem 2.4 to compute $\hat{\lambda}_v(P)$.

According to the theory of the arithmetic-geometric mean, the sequence of curves $(E_n)_n$ converges to a cubic curve

$$E_\infty : y^2 = x(x + M(a,b)^2)^2$$

with a double point, where $M(a,b)$ is the common limit of the sequences $a = (a_n)_n$ and $b = (b_n)_n$. Furthermore, the sequence of points $(P_n)_n = (x_n, y_n)_n$ converges to a point $P_\infty = (x_\infty, y_\infty) \in E_\infty(\mathbb{R})$ and the sequence of isogenies $(\phi_n)_n$ converges to the identity map on $E_\infty(\mathbb{R})$. From (2.3) we get the following limit formula

$$\hat{\lambda}_v(P) = \hat{\lambda}_0(P) = \log \lim_{n\to\infty} \frac{(x_n + a_n^2)^{2^{n-1}}}{\prod_m^{n-1}(x_m + a_m^2)^{2^{m-1}}}. \tag{2.4}$$

Here x_n can be calculated as

$$x_n = \frac{1}{2}\left(x_{n-1} - a_{n-1}b_{n-1} + \sqrt{(x_n + a_n^2)(x_n + b_n^2)}\right).$$

We can use (2.4) to compute $\hat{\lambda}_v(P)$ for a nonzero point $P \in E(\mathbb{R})$ satisfying our various assumptions. If $P \in J(k)$ and v is a real place of k, then we can embed P into $E(\mathbb{R})$, apply some transformations such that the image Q of P under it satisfies the assumptions, compute $\hat{\lambda}(Q)$ and finally use Proposition 2.5 to deduce the value of $\hat{\lambda}_v(P)$.

Notice that the quotient

$$\frac{(x_n + a_n^2)^{2^{n-1}}}{\prod_m^{n-1}(x_m + a_m^2)^{2^{m-1}}}$$

converges quadratically as n goes to ∞. The crucial point is that the sequence of canonical local heights $(\hat{\lambda}_n(P_n))_n$ converges quadratically to $\hat{\lambda}_\infty(P_\infty) = \log|x_\infty + M(a,b)^2|$. Hence this algorithm is faster than the other two methods in theory; more importantly for us, it is also superior in practice, because the operations involved (in particular the square roots) are not too expensive.

Chapter 3

Jacobian surfaces

After the case of elliptic curves had been treated successfully, the next question to ask was whether canonical heights could also be computed explicitly for other abelian varieties. In this context it is natural to first consider Jacobians of curves of genus 2. In the late 1980s and early 1990s Cassels and Flynn embarked on a program to make the arithmetic of curves of genus 2 more explicit, one of the goals being the ability to compute Mordell-Weil groups of Jacobians surfaces with moderately sized coefficients over number fields, see [20]. One of the main tools was the explicit construction of the Kummer surface associated to a Jacobian surface due to Flynn, see [41].

The first algorithm for the computation of the canonical height on Jacobian surfaces, which in fact works entirely on the associated Kummer surface and uses the decomposition into canonical local heights given in Theorem 1.8, was introduced by Flynn and Smart in 1997 in [43]. However, it proved to be infeasible in certain cases. Some modifications to their algorithm were proposed by Stoll in 2002 in [94]. Although this yielded a significant improvement, the situation, especially for non-archimedean places, remained far from the satisfactory state of the available methods for elliptic curves. In this chapter we report on our attempt to improve this situation.

3.1 Jacobian surfaces and Kummer surfaces

In this section we let l denote a field of characteristic $\mathrm{char}(l) \neq 2$. Let

$$F(X,Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

be a binary sextic in $l[X,Z]$ without multiple factors. Then the affine equation

$$Y^2 = F(X,1) \tag{3.1}$$

defines a curve of genus 2 over l and we let C denote its smooth projective model over l. Note that we can find an equation of this form for any curve of genus two defined over l, because of the assumption $\mathrm{char}(l) \neq 2$. We denote the Jacobian variety of C by J. Recall that the Jacobian of a smooth projective curve of genus $g \geq 1$ is an abelian variety of dimension g and that, as a group, it is isomorphic to the kernel of the degree map on the Picard group of C.

In [20, Chapter 2] Cassels and Flynn construct an explicit embedding of the Jacobian into $\mathbb{P}^{15}$, where its image is given as the intersection of 72 quadrics, but in practice it is quite difficult to work with this embedding explicitly.

If we form the quotient of J by the negation map, then we get another classical variety K, the Kummer surface associated with J. The Kummer surface can be embedded into $\mathbb{P}^3$ (as opposed to $\mathbb{P}^{15}$), so explicit calculations

are much more efficient on K than on J. In [40] and [41] Flynn finds an explicit embedding of K into $\mathbb{P}^3$. Since remnants of the group structure are preserved when passing to the Kummer surface, these remnants can be used to obtain a feasible method for performing arithmetic on J.

Explicit embeddings of both the Jacobian and the Kummer surface can be found using a modified version of the classical theta divisor on the Jacobian. The classical theta divisor Θ over an algebraically closed field l is defined to be the divisor on J given by the image of C under the embedding

$$\begin{aligned} \iota : C &\hookrightarrow J \\ P_1 &\mapsto [(P_1) - (\infty)], \end{aligned}$$

where we may assume $f_6 = 0$ because l is algebraically closed, and so we have a unique point ∞ at infinity. If, on the other hand, l is not algebraically closed, then we have to consider the case $f_6 \neq 0$. In that situation there are two branches ∞^+ and ∞^- over the singular point at infinity on the projective closure of the given equation and we define Θ^+ and Θ^- to be the images of C under the embeddings

$$\begin{aligned} \iota^+ : C &\hookrightarrow J \\ P_1 &\mapsto [(P_1) - (\infty^+)] \end{aligned}$$

and

$$\begin{aligned} \iota^- : C &\hookrightarrow J \\ P_1 &\mapsto [(P_1) - (\infty^-)], \end{aligned}$$

respectively. It follows from a theorem of Lefshetz (see for example [58, Chapter VI, Theorem 6.1]) that a basis of the space $\mathcal{L}(2(\Theta^+ + \Theta^-))$ gives a $\mathbb{P}^{15}$ embedding of the Jacobian and a basis of the space $\mathcal{L}(\Theta^+ + \Theta^-)$ gives a $\mathbb{P}^3$ embedding of the Kummer surface. If Θ is the theta divisor corresponding to any fixed l'-rational Weierstrass point, where l' is an extension field of l, then $\mathcal{L}(\Theta^+ + \Theta^-)$ is isomorphic to $\mathcal{L}(2\Theta)$ over l'. All our constructions below continue to work in case $f_6 = 0$.

An l-rational point P on J can be represented by an unordered pair $\{P_1, P_2\}$ where P_1 and P_2 are points on the curve C that are either both defined over l or are defined over a quadratic extension of l and conjugate over l such that $(P_1) + (P_2) - (\infty^+) - (\infty^-)$ or $(P_1) + (P_2) - 2(\infty)$ is in P, viewed as a divisor class on C. If $P \neq 0$, then this representation is unique.

Following the notation from [20], suppose $P_1 = (x, y)$ and $P_2 = (u, v)$ are affine points on the curve such that $x \neq u$. Then a projective embedding

of the Kummer surface is given by

$$\begin{aligned}\kappa_1 &= 1\\ \kappa_2 &= x+u\\ \kappa_3 &= xu\\ \kappa_4 &= \frac{F_0(x,u)-2yv}{(x-u)^2},\end{aligned}$$

where

$$\begin{aligned}F_0(x,u) &= 2f_0+f_1(x+u)+2f_2(xu)+f_3(x+u)xu+2f_4(xu)^2\\ &\quad +f_5(x+u)xu+2f_6(xu)^3.\end{aligned}$$

The values of $\kappa_1(P),\ldots,\kappa_4(P)$ for P not of the form $P=[(x,y)-(u,v)]$ with $x\neq u$ can be found in [43, §2].

The functions $\kappa_1,\kappa_2,\kappa_3,\kappa_4$ satisfy the quartic equation

$$K(\kappa_1,\kappa_2,\kappa_3,\kappa_4)=K_2(\kappa_1,\kappa_2,\kappa_3)\kappa_4^2+K_1(\kappa_1,\kappa_2,\kappa_3)\kappa_4+K_0(\kappa_1,\kappa_2,\kappa_3)=0, \tag{3.2}$$

where

$$\begin{aligned}K_2(\kappa_1,\kappa_2,\kappa_3) &= \kappa_2^2-4\kappa_1\kappa_3,\\ K_1(\kappa_1,\kappa_2,\kappa_3) &= -4\kappa_1^3f_0-2\kappa_1^2\kappa_2f_1-4\kappa_1^2\kappa_3f_2-2\kappa_1\kappa_2\kappa_3f_3-4\kappa_1\kappa_3^2f_4\\ &\quad -2\kappa_2\kappa_3^2f_5-4\kappa_3^3f_6,\\ K_0(\kappa_1,\kappa_2,\kappa_3) &= -4\kappa_1^4f_0f_2+\kappa_1^4f_1^2-4\kappa_1^3\kappa_2f_0f_3-2\kappa_1^3\kappa_3f_1f_3-4\kappa_1^2\kappa_2^2f_0f_4\\ &\quad +4\kappa_1^2\kappa_2\kappa_3f_0f_5-4\kappa_1^2\kappa_2\kappa_3f_1f_4-4\kappa_1^2\kappa_3^2f_0f_6+2\kappa_1^2\kappa_3^2f_1f_5\\ &\quad -4\kappa_1^2\kappa_3^2f_2f_4+\kappa_1^2\kappa_3^2f_3^2-4\kappa_1\kappa_2^3f_0f_5+8\kappa_1\kappa_2^2\kappa_3f_0f_6\\ &\quad -4\kappa_1\kappa_2^2\kappa_3f_1f_5+4\kappa_1\kappa_2\kappa_3^2f_1f_6-4\kappa_1\kappa_2\kappa_3^2f_2f_5\\ &\quad -2\kappa_1\kappa_3^3f_3f_5-4\kappa_2^4f_0f_6-4\kappa_2^3\kappa_3f_1f_6-4\kappa_2^2\kappa_3^2f_2f_6\\ &\quad -4\kappa_2\kappa_3^3f_3f_6-4\kappa_3^4f_4f_6+\kappa_3^4f_5^2.\end{aligned}$$

We let $\kappa:=(\kappa_1,\kappa_2,\kappa_3,\kappa_4)$ be the map from the Jacobian into $\mathbb{P}^3$. Clearly it identifies inverses and is hence 2 to 1, except on points of order 2, where it is injective. Therefore the image of κ is an explicit realization of the Kummer surface K in $\mathbb{P}^3$ given by the defining equation $K(\kappa_1,\kappa_2,\kappa_3,\kappa_4)=0$. Note that when $f_6=0$ the same formulas work.

Definition 3.1. Let l be a field with algebraic closure $\bar{l}$ and let $x=(x_1,x_2,x_3,x_4)\in\mathbb{A}_l^4\setminus\{(0,0,0,0)\}$. Let $K\subset\mathbb{P}_l^3$ be the Kummer surface associated with the Jacobian J of a smooth projective genus 2 curve defined over l. We say that x is a *set of Kummer coordinates on* K if the image of x in $\mathbb{P}_{\bar{l}}^3$ lies on K. If $P\in J$, then we say that x is a *set of Kummer coordinates for* P if x represents $\kappa(P)$, that is, if $\kappa(P)=(x_1:x_2:x_3:x_4)$. The set of all sets of Kummer coordinates on K is defined by

$$K_{\mathbb{A}}:=\{(x_1,x_2,x_3,x_4)\in\mathbb{A}^4:\exists P\in K \text{ such that } P=(x_1:x_2:x_3:x_4)\}$$

Note that $K_{\mathbb{A}}$ equals the set of elements of $\mathbb{A}^4 \setminus \{(0,0,0,0)\}$ satisfying the equation of K. Compare this to the case of an elliptic curve discussed in Section 2.2, where $K_{\mathbb{A}}$ was simply $\mathbb{A}^2 \setminus \{(0,0)\}$.

Now we describe how the group law is reflected on the Kummer surface. First, since a point $Q \in J$ of order 2 is equal to its inverse and κ precisely identifies inverses, addition of $\kappa(Q)$ is well-defined on the Kummer surface K. Furthermore, addition of $\kappa(Q)$ extends to a linear map on $\mathbb{P}^3$ and thus can be written as multiplication by a matrix W_Q.

Second, there is a matrix $B = (B_{ij}(x,y))_{i,j\in\{1,2,3,4\}}$ of biquadratic forms with the following property: Suppose we have Kummer coordinates $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$ for $P, Q \in J$ respectively, then we can choose Kummer coordinates w and z for $P + Q$ and $P - Q$, respectively, satisfying

$$\begin{aligned} B_{ij}(x,y) &= w_i z_j + w_j z_i \quad \text{for } 1 \le i \ne j \le 4 \\ B_{ii}(x,y) &= w_i z_i \quad \text{for } 1 \le i \le 4. \end{aligned}$$

We abbreviate this by

$$w * z = B(x,y). \tag{3.3}$$

Finally, multiplication by 2 is well-defined on the Kummer surface, because duplication commutes with negation – more generally, multiplication by any $n \in \mathbb{Z}$ is well-defined on K. The duplication map can be given by quartic polynomials $\delta_1, \delta_2, \delta_3, \delta_4$ (unique modulo the defining equation of the Kummer surface if we require the normalization condition $\delta((0,0,0,1)) = (0,0,0,1)$ to be satisfied) such that for $P \in J$ we have

$$\kappa(2P) = \delta(\kappa(P)), \tag{3.4}$$

where $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$. Explicit expressions for W_Q, B and δ can be found in [20]. We discuss them in a more general setting in Section 3.3.

3.2 Canonical heights on Jacobian surfaces

3.2.1 Global construction

Let k be a number field or a one-dimensional function field of characteristic $\mathrm{char}(k) \ne 2$ with fixed algebraic closure $\bar{k}$, let C be a curve of genus 2 defined over k and given by the smooth projective model of an affine equation of the form

$$Y^2 = F(X,1),$$

as in (3.1), so $F(X,Z) \in k[X,Z]$ is homogeneous of degree 6 and has no multiple roots in $\mathbb{P}^1_{\bar{k}}$. We may assume without loss of generality that $F(X,Z) \in \mathcal{O}_k[X,Z]$. Let J be the Jacobian of C and K the associated

Kummer surface introduced above. In this section we want to construct canonical heights on J, so according to Theorem 1.3 we first need to pick an ample and symmetric divisor class. The previous section suggests the class of the divisor D_1 as a natural choice, where $D_1 = 2\Theta$ if C has a unique rational point at infinity and $D_1 = \Theta^+ + \Theta^-$ otherwise. Its linear system is base point free and the corresponding morphism to $\mathbb{P}^3$ is given by $\kappa = (\kappa_1, \kappa_2, \kappa_3, \kappa_4)$ defined above.

Definition 3.2. The *naive height on* J is the function on $J(\bar{k})$ defined by

$$h(P) := h_{D_1}(P) = h(\kappa(P)).$$

Furthermore, we call the function $\hat{h} : J(\bar{k}) \longrightarrow \mathbb{R}$ that maps $P \in J(\bar{k})$ to

$$\hat{h}(P) := \hat{h}_{D_1}(P) = \lim_{n\to\infty} \frac{1}{4^n} h\left(2^n P\right).$$

the *canonical height on* J.

We want to decompose the canonical height into a sum of Néron functions as in Theorem 1.8. However, we must take into account that Néron functions associated with a divisor are only defined on points outside the support of the divisor. For $i = 1, 2, 3, 4$ we define

$$D_i := \{P \in J : \kappa_i(P) = 0\} \in \mathrm{Div}(J)(k); \tag{3.5}$$

for $i = 1$ this coincides with our earlier definition. Note that we can find some i such that $P \notin \mathrm{supp}(D_i)$ for every point $P \in J(k)$. In order to use Theorem 1.8 for the computation of the canonical height, it suffices to find canonical local heights $\lambda_{D_i,v}$ associated with D_i, v and g_i for all $i = 1, 2, 3, 4$ and for all $v \in M_k$, where g_i is some fixed function such that $[2]^*(D_i) = 4D_i + \mathrm{div}(g_i)$. In other words, we want to find Néron functions satisfying (1.2) for D_i, g_i and all places v simultaneously.

Remark 3.3. The map κ is analogous to the map κ on an elliptic curve defined in Section 2.2, since both maps identify inverses. The choice of the normalization $(x(P) : 1)$ which is defined for all $P \neq O$ corresponds to the normalization $\kappa(P)/\kappa_1(P)$ and hence to the choice of D_1 is its linear equivalence class.

Let $v \in M_k$ and let C be a smooth projective curve of genus 2 defined over k_v and given as the smooth projective model of an $\mathcal{O}_v$-integral equation (3.1). We adopt the following notation: If $n \geq 1$ and $z = (z_1, \ldots, z_n) \in k_v^n$, then we set

$$v(z) := \min\{v(z_1), \ldots, v(z_n)\}.$$

Definition 3.4. Let $i \in \{1, 2, 3, 4\}$, let $P \in J(k_v) \setminus \mathrm{supp}(D_i)$ and let

$$x = \left(\frac{\kappa_j(P)}{\kappa_i(P)}\right)_{j=1,\ldots,4}.$$

The *naive local height of P associated with D_i and v* is

$$\lambda_{i,v}(P) := -\frac{N_v}{n_v} v(x).$$

Now suppose $P \in J(k_v) \setminus \operatorname{supp}(D_i)$ such that also $2P \notin \operatorname{supp}(D_i)$. Then we find

$$\lambda_{i,v}(2P) - 4\lambda_{i,v}(P) = -\log |g_i(P)|_v - \frac{N_v}{n_v}\varepsilon_v(P), \tag{3.6}$$

where

$$g_i(P) = \delta_i(x)$$

and

$$\varepsilon_v(P) = v(\delta(x)) - 4v(x). \tag{3.7}$$

It is easy to see that we have $[2]^*(D) = 4D + \operatorname{div}(g_i)$ and that ε_v is locally bounded and continuous in the v-adic topology. Moreover, $\varepsilon_v(P)$ does not depend on the normalization x of $\kappa(P)$; we return to this below. Since the coefficients of F and of the δ_i are v-integral, $\varepsilon_v(P)$ is always nonnegative if v is non-archimedean.

From (3.6) we see that $\lambda_{i,v}$ is a Weil function associated with D_i, see Definition 1.4. Using Proposition 1.6, we can define canonical local heights on Jacobian surfaces:

Definition 3.5. Let v be a place of k and fix some $i \in \{1, 2, 3, 4\}$. We call the Néron function

$$\begin{aligned} \hat{\lambda}_{i,v} : J(k_v) \setminus \operatorname{supp}(D_i) &\longrightarrow \mathbb{R} \\ P &\mapsto \frac{N_v}{n_v}(\lambda_{i,v}(P) - \mu_v(P)) \end{aligned}$$

the *canonical local height on J associated with D_i and v*, where

$$\mu_v(P) = \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \varepsilon_v(2^n P).$$

for any $P \in J(k_v)$.

Remark 3.6. Our notation is slightly different from the notation of [43]; namely, our ε_v and μ_v are equal to their functions of the same name, multiplied by -1.

Now suppose that C is defined over k. If $P \in J(k) \setminus \operatorname{supp} D_i$, then

$$h(P) = \sum_{v \in M_k} n_v \lambda_{i,v}(P) \tag{3.8}$$

is obvious.

Furthermore, the next proposition follows immediately from Theorem 1.6 and the construction of $\hat{\lambda}_{i,v}$:

Proposition 3.7. *Suppose $i \in \{1,2,3,4\}$ and $P \in J(k) \setminus \operatorname{supp}(D_i)$. Then we have*

$$\hat{h}(P) = \sum_{v \in M_k} n_v \hat{\lambda}_{i,v}(P).$$

3.2.2 The algorithm of Flynn and Smart

Flynn and Smart have introduced an algorithm for the computation of $\hat{h}(P)$ for $P \in J(k)$, where k is a global field and $\operatorname{char}(k) \neq 2$, in [43]. The first step is to successively compute multiples mP for $m = 1, 2, \ldots$ until we reach some M such that $\varepsilon_v(MP) = 0$ for all non-archimedean places $v \in M_k$.

We assume that k is a global field, because then, according to [20, §7.5], the kernel of reduction at v (with respect to the given model) has finite index in $J(k_v)$ for all non-archimedean v and if MP lies in this kernel, then clearly $\varepsilon_v(MP) = 0$. For each $v \in M_k^0$ we let M_v denote the smallest positive integer such that $\varepsilon_v(M_v P) = 0$. We obviously have $M_v = 1$ for places v of good reduction. Defining M to be the least common multiple of the M_v works. Stoll proves in [94] that $\varepsilon_v(MP) = 0$ implies $\varepsilon_v(2^n MP) = 0$ for all $n \geq 0$ (see Theorem 3.9), thus verifying the correctness of the crucial point of the algorithm, namely the equation

$$\hat{h}(MP) = h(MP) - \sum_{v \in M_k^\infty} \frac{N_v}{n_v} \mu_v(MP). \tag{3.9}$$

In order to compute the right hand side we can pick any set of Kummer coordinates for MP. If $k = \mathbb{Q}$ or, more generally, if k is a number field of class number one, the condition $\varepsilon_v(MP) = 0$ for any $v \in M_k^0$ can be tested easily: We first pick a set of Kummer coordinates $x = (x_1, x_2, x_3, x_4)$ for $\kappa(MP)$ such that $x_1, \ldots, x_4$ are integral and relatively prime. Then the vanishing of $\varepsilon_v(MP)$ for all $v \in M_k^0$ is equivalent to the condition

$$\gcd\big(\delta_1(x), \delta_2(x), \delta_3(x), \delta_4(x)\big) = 1.$$

Supposing that we have succeeded in finding M, we can then proceed to the second step which uses the quadraticity of the canonical height and the identity (3.9) to compute $\hat{h}(P)$:

$$\hat{h}(P) = \frac{1}{M^2}\hat{h}(MP) = \frac{1}{M^2}\left(h(\kappa(MP)) - \sum_{v \in M_k^\infty} \frac{N_v}{n_v} \mu_v(\kappa(MP))\right)$$

Here the computation of $\mu_v(\kappa(MP))$ for archimedean v can be done numerically by computing a large enough number of terms to achieve a desired accuracy; this is similar to the Tate series approach for elliptic curves, see

Section 2.4. But we need to estimate the error, so we need a bound on the local height constant

$$\gamma_v = \sup\{|\varepsilon_v(P)| : P \in J(k_v)\}.$$

Such bounds will be discussed below, see the end of Section 3.2.3.

Also recall that in order to compute $h(MP)$ we can simply pick some i such that $\kappa_i(MP) \neq 0$ and compute $h(P)$ using (3.8) – of course, if k is a number field of class number one, we can find a set of Kummer coordinates for MP with relatively prime entries, so that the non-archimedean contributions to the naive height all vanish.

Remark 3.8. Although their algorithm completely avoids factorisation of integers, which can be quite expensive, it has a significant disadvantage. Namely one has to (globally) compute the points $\kappa(mP)$ and their doubles for all m between 1 and M. However, the size of the coordinates of $\kappa(mP)$ roughly grows like m^2, so for large values of M this algorithm becomes infeasible. See the discussion in the introduction to [94].

3.2.3 Stoll's refinements

In order to tackle the problem just described, Stoll analyzes the map ε_v for non-archimedean v in [94]. The main result is the following theorem.

Theorem 3.9. *(Stoll) Let v be non-archimedean and let C be a smooth projective genus 2 curve given by a model $Y^2 = F(X,1)$, where $F(X,Z) \in \mathcal{O}_v[X,Z]$ is homogeneous of degree 6 and has no multiple factors. Let*

$$U_v := \{P \in J(k_v) : \varepsilon_v(P) = 0\}.$$

Then U_v is a subgroup of $J(k_v)$ and ε_v factors through the quotient $J(k_v)/U_v$. Moreover, $\varepsilon_v(-P) = \varepsilon_v(P)$ and U_v contains the kernel of reduction with respect to the given model. If k is a global field, then U_v has finite index in $J(k_v)$.

Proof. See [94, Theorem 4.1]. □

Notice that since ε_v factors through the Kummer map κ which identifies inverses, the assertion $\varepsilon_v(-P) = \varepsilon_v(P)$ is trivial. The theorem clearly shows $\varepsilon_v(P) = 0 \Rightarrow \varepsilon_v(2P) = 0$. Our Theorem 3.29 will generalize Theorem 3.9.

This theorem is used in [94] to introduce a revised version of the algorithm of Flynn and Smart. The difference is that we compute $\mu_v(P)$ exactly for non-archimedean v and for these computations we only need to find mP for m between 1 and $M' := \max\{M_v : v \in M_k^0\}$. Fix $v \in M_k^0$ such that $\varepsilon_v(P) \neq 0$. We calculate $\varepsilon_v(\kappa(mP))$ for $m = 1, 2, \ldots, M_v$ until $\varepsilon_v(\kappa(M_v P)) = 0$. Then $\mu_v(\kappa(P))$ can be computed exactly as a rational

combination of the $\varepsilon_v(\kappa(mP))$; namely as a finite number of terms plus a finite number of geometric series, see [94, §6].

This revised version has significant advantages over the original algorithm of Flynn and Smart. First, the computations in the second step need not be performed exactly, a suitable finite v-adic precision is sufficient. Second, it only requires the computation of $\varepsilon_v(\kappa(mP))$ for $m = 1, 2, \ldots, M'$, where $M' = \max\{M_v : v \in M_k^0\}$,, in contrast to the original algorithm, which required us to go up to $M = \operatorname{lcm}\{M_v : v \in M_k^0\}$. A more detailed discussion and analysis of the resulting algorithm can be found in [94].

Remark 3.10. If k is a one-dimensional function field that is not a global field (for example $k = l(t)$, where l is some number field), then the above algorithm is still applicable in case we can find an M_v such that $\varepsilon_v(M_v P) = 0$ for a given P. It is an open problem whether we can change the model to ensure that such an M_v can always be found. If this is false in general, one can still ask the same question if we only allow the curve to have certain reduction types at the non-archimedean places. We will return to this question later on in Remark 3.75.

According to Section 1.7 it is not sufficient to be able to compute canonical heights in order to determine the Mordell-Weil group $J(k)$. Indeed, if we want to apply the algorithm introduced in [94, §7] we also need a method to list rational points of naive height up to an upper bound. This upper bound can be decomposed into a certain upper bound on the canonical height and a bound on the difference between the naive and the canonical height. See also Remark 5.14.

Let β be defined by

$$\beta := \sup\left\{ |h(P) - \hat{h}(P)| : P \in J(k) \right\}.$$

We call β the *height constant of* J. Then we have

$$\beta \leq \sum_{v \in M_k} \beta_v,$$

where

$$\beta_v = \sup\left\{ |\mu_v(P)| : P \in J(k_v) \right\}.$$

In order to find an upper bound on β_v, it is sufficient (but not necessary) to find an upper bound on

$$\gamma_v = \sup\left\{ |\varepsilon_v(P)| : P \in J(k_v) \right\},$$

for if B is such a bound, then $B/3$ is clearly an upper bound for β_v. Bounds for the height constant are already presented in [42] and [43]. Stoll improves on this by explicitly bounding the non-archimedean local height constants as follows:

Proposition 3.11. *(Stoll) Let v be non-archimedean. Then we have*

$$\gamma_v \leq -\log |2^4 \operatorname{disc}(F)|_v$$

and hence

$$\beta_v \leq -\log |2^4 \operatorname{disc}(F)|_v / 3.$$

Proof. See [92, Theorem 6.1]. □

Stoll presents several improvements of these bounds in certain cases in [92, §7] and also explains how to obtain bounds for the archimedean local height constants ([92, p. 190]). Further improvements are due to Stoll [94, §5] and Uchida [103, §6].

In this thesis we concentrate on the computation of canonical heights. However, several of our results allow us to improve on the bound on β_v given in Proposition 3.11 and we shall mention these improvements along the way.

Finally, there is a program [96] written by Stoll that searches for rational points of naive height up to a given bound, provided that bound is not too large.

3.2.4 The "kernel" of ε_v

The group $U_v = \{P \in J(k_v) : \varepsilon_v(P) = 0\}$ remains rather mysterious in Theorem 3.9. We present a characterization of U_v when the residue characteristic is not 2 that depends on the choice of model (in $\mathbb{P}^{15}$) of J. The same result is proved independently in [13, Proposition 5.9]. Our proof is based on a case distinction.

Proposition 3.12. *Let k be a number field or one-dimensional function field, let k_v be the completion of k at a non-archimedean place $v \in M_k$ with residue field $\mathfrak{k}$ of characteristic $\operatorname{char}(\mathfrak{k}) \neq 2$ and let $Y^2 = F(X, 1)$ be a model for a smooth projective genus 2 curve C defined over k_v. Let J be the Jacobian of C and let $J^0(k_v)$ denote the points of $J(k_v)$ of non-singular reduction mapping to the component of the identity of the reduction of J, where reduction means reduction with respect to the model consisting of 72 quadratic relations in $\mathbb{P}^{15}$ constructed in [20] and determined by the given model of C. Then we have*

$$U_v = J^0(k_v).$$

In order to prove the proposition, we can assume k_v is strictly Henselian, so $\mathfrak{k}_v$ is algebraically closed. We work over $\mathfrak{k}_v$; the result is an immediate consequence of the following:

No.	F(X,Z)	cond.	add.
1	0	$x_4 = 0$	
2	Z^6	$x_4 = 0$	
3	XZ^5	$x_4 = 0$	$x_1 = 0$
4	X^2Z^4	$x_4 = 0$	
5	X^3Z^3	$x_4 = 0$	$x_1x_3 = 0$
6	$X(X-Z)Z^4$	$x_4 = 0$	$x_1 = 0$
7	$X^2(X-Z)Z^3$	$x_4 = 0$	$x_1x_3 = 0$
8	$X^2(X-Z)^2Z^2$	$x_4 = 0$	
9	$X(X-Z)(X-aZ)Z^3$	$x_1 = x_4 = 0$	
10	$X^2(X-Z)(X-aZ)Z^2$	$x_4 = 0$	$x_1x_3 = 0$
11	$X(X-Z)(X-aZ)(X-bZ)Z^2$	$x_1 = x_4 = 0$	

Table 3.1: Conditions for the vanishing of $\delta(x)$ for orbit representatives

Lemma 3.13. *Let l be an algebraically closed field with* $\mathrm{char}(l) \neq 2$ *and let $F(X,Z) \in l[X,Z]$ be a binary sextic. Let $J_F \subset \mathbb{P}^{15}_l$ be the scheme defined using the 72 quadratic equations from [20, Chapter 2] that define the Jacobian when F is square-free. Let J_F^0 be the component of J_F containing $O = (1:0:\ldots:0)$. Let $K_F \subset \mathbb{P}^3_l$ be the scheme defined by the equation* (3.2)*, let $\kappa : J_F \longrightarrow K_F$ be the map defined in Section 3.1. Finally, let the polynomials δ_i on K_F be also as defined in that section (and given explicitly in [20]) and set $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$. Then we have*

$$\delta(\kappa(P)) \neq (0,0,0,0) \quad \Leftrightarrow \quad P \in J_F^0$$

for all $P \in J_F$.

Proof. It suffices to consider one representative for each orbit of binary sextics under the action $(X:Z) \mapsto (aX+bZ : cX+dZ)$ of $\mathrm{GL}_2(l)$, see the proof of [94, Proposition 3.1]. Table 3.1 is the same as Table 1 of loc. cit. and contains the following information: Representatives for each orbit (column $F(X,Z)$), together with conditions (column cond.) for the simultaneous vanishing of all $\delta_i(x)$, which we abbreviate by $\delta(x) = 0$, where x is a set of Kummer coordinates on K_F (cf. Definition 3.1), and additional conditions (column add.) for a set of coordinates satisfying the conditions to lie on K_F. Notice that here $a, b \notin \{0,1\}$ are distinct and that we can obviously disregard the case of square-free reduction.

Let C_F be given by the equation $Y^2 = F(X,Z)$ in weighted projective space $\mathbb{P}^2_l(1,3,1)$. We use [13, Proposition 5.5] which states that a point $P \in J_F \setminus \{O\}$ is smooth if and only if it is of one of the following two forms:

1. We have $P = [(P_1) - (P_2)]$, where P_1, P_2 are smooth points on C_F.
2. If $(A(X,Z), Y - B(X,Z))$ is the Mumford representation of P (see Section 5.2.2), then $A(X,Z) = cL(X,Z)^2$ has a double root at a multiple

root of F, but L^3 does not divide $F - B^2$.

Furthermore, the point O is always smooth. Note that when $F = 0$ all smooth points of J_F are of the second type.

We first want to show that a point $P \in J_F^0$ satisfies $\delta(\kappa(P)) \neq 0$ if F is one of the 11 orbit representatives from Table 3.1. We have $\kappa(O) = (0 : 0 : 0 : 1)$ and $\delta((0, 0, 0, 1)) = (0, 0, 0, 1)$.

If P is of type 1, then neither P_1 nor P_2 are equal to the singular point at ∞, so $x_1 \neq 0$ and if $X^2 | F(X, Z)$, then we must also have $x_3 \neq 0$. This takes care of the situation where F is not a square. If, on the other hand, $F(X, Z)$ is a square, say $F(X, Z) = G(X, Z)^2$, then we are in case 2, 4 or 8 and $P \in J_F^0 \setminus \{O\}$ means that P_1 and P_2 are affine, lie on the same component and $P_1 \neq P_2$. But for affine P_1, P_2 we can check easily that x_4 is a nonzero multiple of

$$\frac{2G(x_1, 1)G(x_2, 1) + 2y_1y_2}{(x_1 - x_2)^2},$$

where $P_i = (x_i, y_i)$. Hence we have $x_4 = 0$ if and only if P_1 and P_2 lie on different components.

If P is of the second form above, then we can apply a transformation τ to P and F and move the multiple root to ∞. Then $\tau(P)$ satisfies $\kappa(\tau(P)) = (0 : 0 : 1 : x_4)$, where $x_4 \neq c$. But an easy calculation using the equation 3.2 of the Kummer surface reveals that we have $x_4 \neq 0$ as well, and so $\delta(\kappa(P)) \neq 0$, since for our chosen representatives swapping any two multiple roots does not change the necessary condition $x_4 = 0$ for the vanishing of δ.

We still have to show that if $P \in J_F$ is a singular point, then we have $\delta(\kappa(P)) = 0$. For this we observe that a singular point on J_F must map into the singular locus of K_F (but not necessarily vice versa). We define K'_{sing} as follows:

$$K'_{\text{sing}} := \{x \in K : x \text{ is singular, } \delta(x) \neq 0, x \neq (0 : 0 : 0 : 1)\}$$

It suffices to show that, for each of our orbit representatives from Table 3.1, none of the points in K'_{sing} are of the form $\kappa(P)$, where $P \in J_F \setminus J_F^0$. Hence we first compute K'_{sing} for each of these representatives.

1. $K'_{\text{sing}} = \emptyset$
2. $K'_{\text{sing}} = \emptyset$
3. $K'_{\text{sing}} = \emptyset$
4. $K'_{\text{sing}} = \{(1 : 0 : 0 : -1)\}$
5. $K'_{\text{sing}} = \emptyset$
6. $K'_{\text{sing}} = \{(1 : 1 : 0 : 1)\}$

7. $K'_{\text{sing}} = \{(1:0:0:1)\}$
8. $K'_{\text{sing}} = \{(1:0:0:-1), (0:0:1:-1), (1:2:1:-1)\}$
9. $K'_{\text{sing}} = \{(x_1:x_2:0:0), (1:a:0:1), (1:1:0:a), (a:a(1+a):1:0)\}$
10. $K'_{\text{sing}} = \{(1:0:0:-1), (1:0:0:-a), (1:1+a:a:-a)\}$
11. $K'_{\text{sing}} = \{(x_1:x_2:0:0), (1:0:0:ab), (1:a+b:ab:ab), (1:a+1:a:ab), (1:b+1:b:ab), (0:1:1:1), (0:1:a:a^2), (0:1:b:b^2)\}$

Suppose that $x = \kappa(P)$ lies in K'_{sing}. Furthermore, suppose $x_1 \neq 0$ if Z is the only multiple factor of $F(X,Z)$ and $x_1 x_3 \neq 0$ if X^2Z^2 divides $F(X,Z)$. Then P must lie in J_F^0.

It is easy to show that if $x = \kappa(P)$ is of the form $x = (1:0:0:-f_2)$ if $f_0 = f_1 = 0$ or of the form $x = (0:0:1:-f_4)$ if $f_5 = f_6 = 0$, then P is a smooth ramification point of κ. Moreover, we can apply a transformation to the point $(1:2:1:-1)$ in case 8 to put it into either one of these two forms without changing F.

This takes care of all cases, except for case 11, where the points $(0:1:1:1), (0:1:a:a^2), (0:1:b:b^2)$ remain to be considered. Let x be one of these points. Then Z must divide $A(X,Z)$, since $x_1 = 0$ holds. Actually we must have $Z^2 | A(X,Z)$, since otherwise x would have to satisfy $x_4 = 0$, using the explicit description of κ for such points given in [43, §2].

But if P were not smooth, then Z^3 would have to divide $F - B^2$, that is

$$B^2 = -abXZ^5 + (b + a(b+1))X^2Z^4 + \dots$$

which is impossible. Hence P must be smooth, if it exists, and the proof is finished.

□

3.3 Kummer surfaces for general models

It would be desirable to improve the computation of the non-archimedean μ_v by coming up with an algorithm that does not require the computation of points $\kappa(mP)$ on the Kummer surface for large m at all. Ideally, we would like to use an approach similar to Theorem 2.17 which relies on the explicit knowledge of the different possible reduction types of an elliptic curve at v. However, one problem is that if the residue characteristic at v is equal to 2, then models of the form $Y^2 = F(X,1)$ always have bad reduction and are often not minimal at v.

Hence we want to generalize Flynn's construction of the Kummer surface to the case of a genus 2 curve defined over a field l of arbitrary characteristic. For this we need to consider affine defining equations of the form

$$Y^2 + H(X,1)Y = F(X,1), \tag{3.10}$$

where

$$F(X,Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

and

$$H(X,Z) = h_0Z^3 + h_1XZ^2 + h_2X^2Z + h_3X^3$$

are binary forms of degrees 6 and 3, respectively, in $l[X,Z]$. This defines an affine part of a smooth projective curve of genus 2 if and only if the discriminant Δ of the model does not vanish. The discriminant of such a model is defined in [66] and [63]. If the characteristic of l is not equal to 2, we have $\Delta = 2^{-12}\operatorname{disc}(4F + H^2)$. Note that we can find an equation of this form for any smooth projective curve of genus 2, see for instance [20].

3.3.1 Embedding the Kummer surface in arbitrary characteristic

Suppose that we have an equation of the form (3.10) with nonzero discriminant, let C be its smooth projective model over l and let J denote its Jacobian.

Remark 3.14. The results of this section have been obtained independently by Duquesne in the special case $\operatorname{char}(l) = 2$ and $h_3 = 0$, see [33]. He was interested in cryptographic applications and indeed one can use the results obtained in the present section in this context, see [34]. All of our results specialize to his whenever $\operatorname{char}(l) = 2$ and $h_3 = 0$ and they specialize to Flynn's original results whenever we have $\operatorname{char}(l) \neq 2$ and $H = 0$. The content of this section has been published in [73]. Explicit formulas and several Magma routines will be made available on the author's webpage [74].

The first obvious task is to find the map $\kappa : J \longrightarrow \mathbb{P}^3$ in the general case. As in [41] we want to find a basis for the 4-dimensional vector space $\mathcal{L}(D_1)$, where $D_1 = 2\Theta$ if there is a unique rational point at infinity on C and $D_1 = \Theta^+ + \Theta^-$ otherwise, since such a basis must give the desired map $\kappa : J \longrightarrow \mathbb{P}^3$. Suppose we have a generic point $P \in J$ represented by an unordered pair $\{P_1, P_2\}$, where $P_1 = (x,y)$, $P_2 = (u,v)$ and $x \neq u$. A basis may be found by looking for four linearly independent functions on J which are symmetric in P, Q, have a pole of order at most 1 at infinity and may have a pole of any order at $0 \in J$, but are regular elsewhere. As in [41], 3

members of such a basis are easily found, namely the symmetric polynomials in x and u given by $\kappa_1 = 1, \kappa_2 = x + u$ and $\kappa_3 = xu$.

Looking for a suitable fourth coordinate, the following basis can be found:

$$\kappa_1 = 1,\ \kappa_2 = x + u,\ \kappa_3 = xu,\ \kappa_4 = \frac{F_0(x,u) - 2yv - H(x,1)v - H(u,1)y}{(x-u)^2}.$$

This obviously specializes to the basis given in Section 3.1 in the case $H = 0$ and it also specializes to the basis introduced in [33] when $\mathrm{char}(l) = 2$ and $h_3 = 0$. All of these are elements of $\mathcal{L}(D_1)$, because they are even, symmetric, have no pole except at infinity, and grow at worst like xu at infinity. We have a basis, because these 4 elements of the 4-dimensional vector space $\mathcal{L}(D_1)$ are obviously linearly independent.

Similar to the classical case, these $\kappa_1, \kappa_2, \kappa_3, \kappa_4$ satisfy the quartic equation

$$K(\kappa_1,\kappa_2,\kappa_3,\kappa_4) = K_2(\kappa_1,\kappa_2,\kappa_3)\kappa_4^2 + K_1(\kappa_1,\kappa_2,\kappa_3)\kappa_4 + K_0(\kappa_1,\kappa_2,\kappa_3) = 0, \tag{3.11}$$

where

$$\begin{aligned}
K_2(\kappa_1,\kappa_2,\kappa_3) &= \kappa_2^2 - 4\kappa_1\kappa_3,\\
K_1(\kappa_1,\kappa_2,\kappa_3) &= -4f_2\kappa_1^2\kappa_3 - 4f_6\kappa_3^3 - 4f_0\kappa_1^3 - h_1h_3(\kappa_2^2\kappa_3 - 2\kappa_1\kappa_3^2)\\
&\quad - h_2h_3\kappa_2\kappa_3^2 - h_1h_2\kappa_1\kappa_2\kappa_3 - h_1^2\kappa_1^2\kappa_3 - 2f_3\kappa_1\kappa_2\kappa_3 - h_0^2\kappa_1^3\\
&\quad - h_2^2\kappa_1\kappa_3^2 - 2f_5\kappa_2\kappa_3^2 - h_3^2\kappa_3^3 - 4f_4\kappa_1\kappa_3^2 - 2f_1\kappa_1^2\kappa_2\\
&\quad - h_0h_1\kappa_1^2\kappa_2 - h_0h_2(\kappa_1\kappa_2^2 - 2\kappa_1^2\kappa_3) - h_0h_3(\kappa_2^3 - 3\kappa_1\kappa_2\kappa_3),\\
K_0(\kappa_1,\kappa_2,\kappa_3) &= (-4f_0f_2 - f_0h_1^2 + f_1^2 + f_1h_0h_1 - f_2h_0^2)\kappa_1^4\\
&\quad + (-4f_0f_3 - 2f_0h_1h_2 + f_1h_0h_2 - f_3h_0^2)\kappa_1^3\kappa_2\\
&\quad + (2f_0h_1h_3 - 2f_1f_3 - f_1h_0h_3 - f_1h_1h_2 + 2f_2h_0h_2\\
&\qquad - f_3h_0h_1)\kappa_1^3\kappa_3\\
&\quad + (-4f_0f_4 - 2f_0h_1h_3 - f_0h_2^2 + f_1h_0h_3 - f_4h_0^2)\kappa_1^2\kappa_2^2\\
&\quad + (4f_0f_5 + 2f_0h_2h_3 - 4f_1f_4 - f_1h_1h_3 - f_1h_2^2 + 2f_2h_0h_3\\
&\qquad + f_3h_0h_2 - 2f_4h_0h_1 + f_5h_0^2)\kappa_1^2\kappa_2\kappa_3\\
&\quad + (-4f_0f_6 - f_0h_3^2 + 2f_1f_5 + f_1h_2h_3 - 4f_2f_4 - f_2h_2^2 + f_3^2\\
&\qquad + f_3h_0h_3 + f_3h_1h_2 - f_4h_1^2 + f_5h_0h_1 - f_6h_0^2)\kappa_1^2\kappa_3^2\\
&\quad + (-4f_0f_5 - 2f_0h_2h_3 - f_5h_0^2)\kappa_1\kappa_2^3\\
&\quad + (8f_0f_6 + 2f_0h_3^2 - 4f_1f_5 - 2f_1h_2h_3 + f_3h_0h_3 - 2f_5h_0h_1\\
&\qquad + 2f_6h_0^2)\kappa_1\kappa_2^2\kappa_3\\
&\quad + (4f_1f_6 + f_1h_3^2 - 4f_2f_5 - 2f_2h_2h_3 + f_3h_1h_3\\
&\qquad + 2f_4h_0h_3 - f_5h_0h_2 - f_5h_1^2 + 2f_6h_0h_1)\kappa_1\kappa_2\kappa_3^2\\
&\quad + (-2f_3f_5 - f_3h_2h_3 + 2f_4h_1h_3 - f_5h_0h_3 - f_5h_1h_2
\end{aligned}$$

$$
\begin{aligned}
&\quad + 2f_6h_0h_2)\kappa_1\kappa_3^3 \\
&+ (-4f_0f_6 - f_0h_3^2 - f_6h_0^2)\kappa_2^4 \\
&+ (-4f_1f_6 - f_1h_3^2 - 2f_6h_0h_1)\kappa_2^3\kappa_3 \\
&+ (-4f_2f_6 - f_2h_3^2 + f_5h_0h_3 - 2f_6h_0h_2 - f_6h_1^2)\kappa_2^2\kappa_3^2 \\
&+ (-4f_3f_6 - f_3h_3^2 + f_5h_1h_3 - 2f_6h_1h_2)\kappa_2\kappa_3^3 \\
&+ (-4f_4f_6 - f_4h_3^2 + f_5^2 + f_5h_2h_3 - f_6h_2^2)\kappa_3^4.
\end{aligned}
$$

The zero locus of $K(\kappa_1, \kappa_2, \kappa_3, \kappa_4)$ gives an explicit realization of the Kummer surface associated with J. It is compatible with the other known results, see Remark 3.14.

Now our task is to find the maps on the Kummer surface which make it so useful for explicit computations, namely the duplication map δ, the matrix of biquadratic forms B and the matrix W that corresponds to translation by a point of order 2.

3.3.2 Duplication

We first determine the duplication map $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ on the Kummer surface K embedded in $\mathbb{P}^3$, see (3.4). Here $\delta_1, \delta_2, \delta_3, \delta_4$ are quartic polynomials in $\kappa_1, \kappa_2, \kappa_3, \kappa_4$ and δ makes the following diagram commute:

$$
\begin{array}{ccc}
J & \xrightarrow{[2]} & J \\
\downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\
K & \xrightarrow{\delta} & K,
\end{array}
$$

where [2] denotes the multiplication-by-2 map on the Jacobian.

In the classical case, Flynn used the biquadratic forms described in the next section to obtain the duplication map. This is possible in the present situation (and gives the same result), but we can also use a different approach that does not depend on the biquadratic forms. We temporarily assume that l is a field of characteristic not equal to 2, so that we can find a simpler model C' for our curve C given by

$$Y^2 = 4F(X, 1) + H(X, 1)^2.$$

Let J' denote its Jacobian and let K' denote its Kummer surface. Then clearly J and J' are isomorphic, as are K and K'. If we can explicitly determine the isomorphism

$$\tau : K \xrightarrow{\cong} K'$$

induced by the isomorphism $C \cong C'$, we can use the following commutative diagram, where δ' denotes the duplication map on K':

$$\begin{array}{ccc} K & \xrightarrow{\delta} & K \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ K' & \xrightarrow{\delta'} & K' \end{array}$$

It is easy to find the isomorphism τ, in fact a short calculation shows that it is given by

$$\begin{array}{rcl} \tau : K & \to & K' \\ (x_1 : x_2 : x_3 : x_4) & \mapsto & (x_1 : x_2 : x_3 : 4x_4 - 2(h_0h_2x_1 + h_0h_3x_2 + h_1h_2x_3)) \,. \end{array}$$

This is a rather easy example of a more general formula, see the discussion following Proposition 3.24 below. Thus we can find δ as

$$\delta := \tau \circ \delta' \circ \tau^{-1}.$$

Notice that this construction is only valid for characteristic $\neq 2$, so in order for the result to remain valid in the remaining case, we want the polynomials δ_i to be defined and remain non-trivial modulo 2. Unfortunately this is not the case, but we can use the fact that the duplication map is only defined modulo the defining polynomial $K(\kappa_1, \kappa_2, \kappa_3, \kappa_4)$ and hence we can add multiples of this polynomial to the δ_i. We do not change δ_1 and δ_3, but we add $-(32h_0h_3 + 32h_1h_2)K(\kappa_1, \kappa_2, \kappa_3, \kappa_4)$ to δ_2 and $(48h_0h_1h_2h_3 + 48h_0^2h_3^2 + 32h_0h_3f_3)K(\kappa_1, \kappa_2, \kappa_3, \kappa_4)$ to δ_4. After dividing all the δ_i by 64 we obtain polynomials, also called $\delta_1, \delta_2, \delta_3, \delta_4$, that are defined and remain non-trivial modulo 2.

Proposition 3.15. *The map δ constructed above represents duplication on the Kummer surface in any characteristic.*

Proof. We only need to show that the map $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ represents duplication in characteristic 2. Since this is a geometric statement, we may as well assume that we have a field l of characteristic 2 that is algebraically closed. Let $W(l)$ be its ring of Witt vectors with field of fractions l'. Let $\widetilde{C}$ denote a genus 2 curve over l, given by the smooth projective model of an equation

$$y^2 + \widetilde{H}(x, 1)y = \widetilde{F}(x, 1)$$

where $F, H \in l[X, Z]$ are homogeneous of degrees 6 and 3, respectively, with Jacobian $\widetilde{J}$ and Kummer surface $\widetilde{K}$. Then $\widetilde{K}$ lifts to a Kummer surface K of a Jacobian J over l'. Let δ denote the duplication map on K that we have just found, reducing to the well-defined, non-trivial map $\widetilde{\delta}$ on $\widetilde{K}$. Let $\widetilde{P} \in \widetilde{J}$, lifting to $P \in J$. Then

$$\delta(\kappa(P)) = \kappa(2P)$$

and so if we normalize $\kappa(P)$ such that the entries lie in $W(l)$ with one of them having valuation zero, then either we have

$$\widetilde{\delta}(\widetilde{\kappa}(\widetilde{P})) = \widetilde{\kappa}(2\widetilde{P})$$

or $\widetilde{\delta}_1(\widetilde{\kappa}(\widetilde{P})) = \ldots = \widetilde{\delta}_4(\widetilde{\kappa}(\widetilde{P})) = 0$. This can be seen by viewing δ and $\widetilde{\delta}$ as maps on the respective $\mathbb{P}^3$'s. We need to show that the latter case cannot occur.

For this we first reduce to a few simple cases. We use a change of model so that, depending on the number of roots of $H(X, Z)$, we are in one of the following three situations:

(a) $H = Z^3$

(b) $H = XZ^2$

(c) $H = X^2Z + XZ^2$

Next, we can use another suitable transformation $Y \mapsto Y + U(X, Z)$ where $U(X, Z)$ is a binary cubic, see (3.16). It is not difficult to see that we can reduce to the case where

$$f = f_1x + f_3x^3 + f_5x^5.$$

The condition that C is nonsingular means in the respective cases:

(a) $f_5 \neq 0$

(b) $f_1f_5 \neq 0$

(c) $f_1f_5(f_1 + f_3 + f_5 + f_1^2 + f_3^2 + f_5^2) \neq 0$

For each of these cases let $x = (x_1, x_2, x_3, x_4) \in l^4$ be a quadruple that satisfies the defining equation $\widetilde{K}(x) = 0$ of the Kummer surface associated to the Jacobian of C. We can use elementary methods, quite similar to those used to prove [94, Proposition 3.1], to show the following.

Lemma 3.16. *If $\widetilde{\delta}_i(x) = 0$ for all $i \in \{1, 2, 3, 4\}$, then we must already have $x_i = 0$ for all $i \in \{1, 2, 3, 4\}$.*

This means that the quadruple does not define a point on the Kummer surface and so the map $\widetilde{\delta}$ represents the duplication map on K. Since the proofs are not very enlightening but rather lengthy, they are not given here but may be found in Appendix A.1. □

3.3.3 Biquadratic forms

Let $P, Q \in J$ and let x, y be Kummer coordinates for P and Q, respectively. Addition on the Jacobian does not descend to give a well-defined addition map on the Kummer surface. Indeed, given x and y, we can find Kummer coordinates of $\kappa(P+Q)$ and $\kappa(P-Q)$, but in general we cannot tell them apart. Instead we can deduce from classical identities of theta functions (see [54]) that

$$\kappa_i(P+Q)\kappa_j(P-Q) + \kappa_j(P+Q)\kappa_i(P-Q)$$

is biquadratic in $(x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)$ for any $i, j \in \{1, 2, 3, 4\}$ and therefore there is a matrix $B := (B_{ij})_{i,j\in\{1,2,3,4\}}$ of biquadratic forms in x, y having the property that there are Kummer coordinates w and z for $P+Q$ and $P-Q$, respectively, such that we have

$$w * z = B(x, y).$$

Recall from (3.3) that we use this notation to abbreviate

$$\begin{aligned} B_{ij}(x, y) &= w_i z_j + w_j z_i \text{ for } i \neq j \\ B_{ii}(x, y) &= w_i z_i, \end{aligned}$$

For the computation of B we again use the fact that the Kummer surface K is isomorphic to K' defined in the last section. The isomorphism $\tau : K \longrightarrow K'$ was also given there.

Let B' denote the corresponding matrix of biquadratic forms on K' and let $x' = \tau(x), y' = \tau(y), z' = \tau(z), w' = \tau(w)$, so that we have

$$w' * z' = B'(x', y'). \tag{3.12}$$

Notice that for $i \in \{1, 2, 3\}$, we have $x'_i = x_i, y'_i = y_i, z'_i = z_i, w'_i = w_i$. We use this fact, our explicit expression of the isomorphism τ and (3.12) to find the matrix B in terms of the entries of B'. We write b'_{ij} for $B'_{ij}(x', y')$.

For $i, j \in \{1, 2, 3\}$ we have

$$B_{ij}(x, y) = w_i z_j + w_j z_i = w'_i z'_j + w'_j z'_i = b'_{ij}.$$

and for $i \in \{1, 2, 3\}$ we have

$$B_{ii}(x, y) = w_i z_i = w'_i z'_i = b'_{ii}.$$

To find an entry of the fourth column (or row) of B not equal to $b'_{4,4}$ we have to do some algebra. We get, for example,

$$B_{1,4}(x, y) = \frac{1}{4} b'_{1,4} + \frac{1}{2} \left(2h_0 h_2 b'_{1,1} + h_0 h_3 b'_{1,2} + h_1 h_3 b'_{1,3} \right)$$

and analogous formulas for $B_{2,4}(x,y)$ and $B_{3,4}(x,y)$. Finally we compute

$$\begin{aligned} B_{4,4}(x,y) &= \frac{1}{4}\left(h_0h_2b'_{1,4}+h_0h_3b'_{2,4}+h_1h_3b'_{3,4}+h_0^2h_2^2b'_{1,1}+h_0^2h_3^2b'_{2,2}\right) \\ &\quad +h_1^2h_3^2b'_{3,3}+\frac{1}{8}\left(h_0^2h_2h_3b'_{1,2}+h_0h_1h_2h_3b'_{1,3}+h_0h_1h_3^2b'_{2,3}\right) \\ &\quad +\frac{1}{16}b'_{4,4}. \end{aligned}$$

Dividing all entries of the matrix thus computed by 16, we obtain a matrix B whose entries are all defined and remain non-trivial modulo 2.

Proposition 3.17. *We have*

$$w * z = B(x,y)$$

in any characteristic.

Proof. As in the previous section, we are required to verify that this matrix actually contains the biquadratic forms we were looking for in case of a field l of characteristic 2. Keeping the notation from Section 3.3.2, we let $\widetilde{B_{ij}}$ denote the reduction of the biquadratic form B_{ij} on a Kummer surface K over the fraction field l' of the ring of Witt vectors reducing to $\widetilde{K}$. Viewing the B_{ij} and the $\widetilde{B_{ij}}$ as maps on $\mathbb{P}^3_{l'}\times\mathbb{P}^3_{l'}$ and $\mathbb{P}^3_{l}\times\mathbb{P}^3_{l}$, respectively, we see that for a given point $(x,y)=((x_1:x_2:x_3:x_4),(y_1:y_2:y_3:y_4))\in\widetilde{K}^3\times\widetilde{K}^3$ either all $\widetilde{B_{ij}}(x,y)$ vanish or they give the correct biquadratic forms.

The proof of the proposition is completed by the following lemma:

Lemma 3.18. *If $x=(x_1,x_2,x_3,x_4)\in l^4$ and $y=(y_1,y_2,y_3,y_4)\in l^4$ satisfy $\widetilde{K}(x)=\widetilde{K}(y)=0$ and if all $\widetilde{B_{ij}}(x,y)$ vanish, then $x_i=0$ for all i or $y_i=0$ for all i.*

By the discussion in Section 3.3.2 we can reduce to the cases (a), (b) and (c) introduced there. The proofs for these cases can be found in Appendix A.2. Note that the methods are again similar to those employed in the proof of [94, Proposition 2.1]; they consist of straightforward, but tedious, algebraic manipulations. □

3.3.4 Translation by a point of order 2

Let $Q\in J$ be a point of order 2. Then we have $P+Q=P-Q$ for all $P\in J$ and translation by $\kappa(Q)$ is defined on the Kummer surface. In fact, it is a linear map on $\mathbb{P}^3$, so it can be given as a matrix in terms of the coefficients of the curve as described in Section 3.1. This matrix was found in the special case $H=0$ by Flynn in [41] and is given in terms of the coefficients of polynomials s and t, where $F(X,1)=s(X)t(X)$, $\deg(s)=2$, $\deg(t)=4$ and

the roots of s are the x-coordinates of the points Q_1, Q_2 on the curve C such that Q can be represented by the unordered pair $\{Q_1, Q_2\}$. Furthermore, the map is an involution and hence the square of the matrix representing it is a scalar multiple of the identity matrix.

As before, we make use of the isomorphism $\tau : K \longrightarrow K'$ in the case $\mathrm{char}(l) \neq 2$. Let $W'_{\tau(Q)}$ denote the matrix corresponding to translation by $\tau(\kappa(Q))$ on K'. We want to find the matrix W_Q that makes the following diagram commute

$$\begin{array}{ccc} K & \xrightarrow{W_Q} & K \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ K' & \xrightarrow{W'_{\tau(Q)}} & K', \end{array}$$

where the horizontal maps denote multiplication by the respective matrix. This means that we express the resulting matrix in terms of the coefficients of polynomials s, t such that $4F(X,1) + H(X,1)^2 = s(X)t(X)$. First we compute

$$W_Q := T^{-1} W'_{\tau Q} T,$$

where T is the matrix corresponding to τ. Then W_Q has the desired properties for $\mathrm{char}(l) \neq 2$.

In order to generalize W_Q to arbitrary characteristic, one could try to manipulate the entries directly, or one could first express them in terms of the Kummer coordinates of Q, as opposed to the coefficients of s and t. Unfortunately, neither of these approaches has proved successful, see the discussion below. Therefore, we have to use a different method. Our approach is analogous to the one used by Flynn in the case where $\mathrm{char}(l) \neq 2$ and $H = 0$. In addition, it is identical with the method used independently by Duquesne in the case where $\mathrm{char}(l) = 2$ and h has degree 2. However, the matrix computed there only works when $\kappa_1(Q) \neq 0$.

Suppose that C is a smooth projective curve of genus 2 given by an affine equation

$$C : Y^2 + H(X,1)Y = F(X,1)$$

and defined over a field l of characteristic equal to 2. Let Q be a l-rational point of order 2 on its Jacobian J. In order to find the matrix W_Q corresponding to translation by Q, we directly compute the image of $P + Q$ on the Kummer surface using the geometric group law on the Jacobian, where $P \in J(l)$ is generic. We then make it linear in the Kummer coordinates of P by simplifying the resulting expression.

The point Q can be represented as $\{Q_1, Q_2\}$ with points $Q_i \in C$. First we assume that Q_1 and Q_2 are affine points, so we have $Q_i = (x_i, y_i)$ and

$$H(x,1) = (x - x_1)(x - x_2)t(x),$$

where $t(x) = t_0 + t_1 x$.

We keep the discussion of this case brief (see [33] or [41] for a more detailed discussion). We first find the top three three rows of the matrix W_Q such that $W_Q\kappa(P) = \kappa(P+Q)$; the last row is computed using the fact that W_Q^2 must be a scalar multiple of the identity matrix. After a little simplification the matrix can be expressed in terms of the Kummer coordinates k_1, k_2, k_3, k_4 of Q and the coefficients of the polynomials f, t and b, where $y = b(x) = b_1 + b_0 x$ is the line joining the points Q_1 and Q_2, so

$$b_0 = \frac{y_1 - y_2}{x_1 - x_2}, \quad b_1 = \frac{x_2 y_1 - x_1 y_2}{x_1 - x_2}.$$

Recall that a point on the Jacobian can be given in Mumford representation as $(a(x), y - b(x))$, where $a(x) = (x - x_1)(x - x_2) = x^2 - \frac{k_2}{k_1}x + \frac{k_3}{k_1}$ (see also Section 5.2.2).

To complete the picture, we have to find the matrix W_Q in the case where $Q_1 = (x_1, y_1)$ is affine and Q_2 is at infinity. Then $b(x)$ is a cubic polynomial. Its leading coefficient r_6 plays the role of the y-coordinate of Q_2 and we can decide which point at infinity Q_2 is using the value of r_6. By going through the same steps as before, we find W_Q in terms of r_6, y_1, the coefficients of f and t and the Kummer coordinates of Q.

In order to unify the two matrices, the following notation is convenient: We set $k_i' := k_i/k_2$ in both cases. If Q_2 is affine we set

$$\begin{aligned}
b_0' &:= \frac{y_1 - y_2}{(x_1 - x_2)^2} = \frac{b_0}{x_1 - x_2}, \\
b_1' &:= \frac{y_1 x_2 - y_2 x_1}{(x_1 - x_2)^2} = \frac{b_1}{x_1 - x_2}, \\
b_2' &:= \frac{y_1 x_2^2 - y_2 x_1^2}{(x_1 - x_2)^2} = b_1' \frac{k_2'}{k_1'} + b_0' \frac{k_3'}{k_1'}, \\
b_3' &:= \frac{y_1 x_2^3 - y_2 x_1^3}{(x_1 - x_2)^2} = b_2' \frac{k_2'}{k_1'} + b_1' \frac{k_3'}{k_1'} = b_1' \left(\frac{k_2'}{k_1'}\right)^2 + b_1' \frac{k_3'}{k_1'} + b_0' \frac{k_2' k_3'}{k_1'^2}, \\
c &:= \frac{y_1 y_2}{x_1 - x_2} = b_0' b_1' \left(\frac{k_2'}{k_1'}\right)^3 + \frac{F(x_1, 1)x_2 + F(x_2, 1)x_1}{x_1 - x_2}.
\end{aligned}$$

Now suppose that Q_2 is at infinity. In this situation we set

$$\begin{aligned}
b_i' &:= r_6 k_3'^i \text{ for } i = 0, 1, 2, \\
b_3' &:= r_6 k_3'^3 + y_1, \\
c &:= y_1 r_6.
\end{aligned}$$

Here y_1 satisfies $y_1^2 = F(x_1, 1)$, hence it can be computed using the coefficients of F and the k_i', or as $y_1 = b(x_1)$.

The unified matrix is given by

$$W_Q = \begin{pmatrix} t_1b'_2 + k'_4 & t_1b'_1 + f_5k'_3 & t_1b'_0 + f_5k'_2 & k'_1 \\ t_0b'_2 + t_1b'_3 + f_3k'_3 & t_0b'_1 + t_1b'_2 + k'_4 & t_0b'_0 + t_1b'_1 + f_3k'_1 & k'_2 \\ t_0b'_3 + f_1k'_2 & t_0b'_2 + f_1k'_1 & t_0b'_1 + k'_4 & k'_3 \\ W_{4,1} & W_{4,2} & W_{4,3} & k'_4 \end{pmatrix},$$

where

$$\begin{aligned} W_{4,1} &= t_0f_1b'_0 + t_0f_3b'_2 + t_0^2c + t_1f_1b'_1 + f_3f_1k'_1, \\ W_{4,2} &= t_0f_5b'_3 + t_0t_1c + t_1f_1b'_0 + f_1f_5k'_2, \\ W_{4,3} &= t_0f_5b'_2 + t_1f_3b'_1 + t_1f_5b'_3 + t_1^2c + f_3f_5k'_3. \end{aligned}$$

It seems curious that our results in this section apparently cannot be combined to form a matrix that works in arbitrary characteristic. One possible reason for this is the fact that if $\mathrm{char}(l) = 2$, then an affine point (x, y) invariant under the hyperelliptic involution satisfies $H(x, 1) = 0$ and if $\mathrm{char}(l) \neq 2$, then such a point satisfies $y = 0$. In general, we can only assume that $2y + H(x, 1) = 0$ and this is not a sufficient simplification to make the method used above work. Moreover, if $\mathrm{char}(l) = 2$, then, depending on the number of distinct roots of $H(x, 1)$, we have $\#J[2] \in \{1, 2, 4\}$, whereas otherwise $\#J[2] = 16$. It would be interesting to find out whether there is a matrix W_Q representing translation by a point of order 2 in arbitrary characteristic, either by finding such a matrix or by proving that it cannot exist.

3.4 Local heights on Kummer coordinates for general models

3.4.1 Definitions and first properties

Now we return to our setup of a number field or one-dimensional function field k. Let v be a place of k and consider a smooth projective genus 2 curve C over k_v given as the smooth projective model of an equation

$$Y^2 + H(X, 1)Y = F(X, 1), \tag{3.13}$$

where

$$F(X, Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

and

$$H(X, Z) = h_0Z^3 + h_1XZ^2 + h_2X^2Z + h_3X^3$$

are binary forms of degrees 6 and 3, respectively, such that the discriminant $\Delta(C)$ is nonzero. We can assume without loss of generality that $F, H \in \mathcal{O}_v[X, Z]$.

We now generalize the definitions of ε_v and μ_v (see (3.7) and Definition 3.5, respectively) to include the present case. Let J denote the Jacobian of C and let K be its Kummer surface discussed in Section 3.3. We let δ and $B = (B_{ij})_{i,j}$ denote the objects defined on K in that section and generalize the notion of Kummer coordinates and of $K_{\mathbb{A}}$ introduced in Section 3.1 to the general case in the obvious way. The following definition is similar to Definition 2.7.

Definition 3.19. Let $x \in K_{\mathbb{A}}(k_v)$ be a set of Kummer coordinates on K. Then we set

$$\varepsilon_v(x) := v(\delta(x)) - 4v(x)$$

and

$$\mu_v(x) = \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \varepsilon_v(\delta^{\circ n}(x)).$$

We recall some of the properties of these functions, since they continue to hold in this more general setting. If x and x' represent the same point in $K(k_v)$, then we have $\varepsilon_v(x) = \varepsilon_v(x')$ and $\mu_v(x) = \mu_v(x')$, and so we can define ε_v and μ_v on $K(k_v)$. If $P \in J(k_v)$, then we define

$$\varepsilon_v(P) := \varepsilon_v(x) \text{ and } \mu_v(P) := \mu_v(x)$$

for any set of Kummer coordinates x for $\kappa(P) \in K(k_v)$.

We will also have occasion to use the following function: Let $x, y \in K_{\mathbb{A}}(k_v)$ and define

$$\varepsilon_v(x, y) := v(B(x, y)) - 2v(x) - 2v(y).$$

If $P, Q \in J(k_v)$, then we have $\varepsilon_v(x, y) = \varepsilon_v(x', y')$ for any sets of Kummer coordinates x, x' for P and y, y' for Q, respectively. Hence we can set

$$\varepsilon_v(P, Q) := \varepsilon_v(x, y) \tag{3.14}$$

for any sets of Kummer coordinates x and y for P and Q, respectively. This was first defined in [94].

Lemma 3.20. *Let $x, y, w, z \in K_{\mathbb{A}}(k_v)$ be Kummer coordinates on K satisfying $w * z = B(x, y)$. Then we have*

$$\delta(w) * \delta(z) = B(\delta(x), \delta(y)).$$

Proof. The proof carries over verbatim from the proof of [94, Lemma 3.2]. □

Corollary 3.21. *Let $x, y, w, z \in K_{\mathbb{A}}(k_v)$ be Kummer coordinates on K satisfying $w * z = B(x, y)$. Then we have*

$$\varepsilon_v(\delta(x), \delta(y)) + 2\varepsilon_v(x) + 2\varepsilon_v(y) = \varepsilon_v(w) + \varepsilon_v(z) + 4\varepsilon_v(x, y).$$

We now refine the notion of the canonical local height. The idea, which is due to Stoll and was first introduced in the unpublished manuscript [95], is to define canonical local heights not for points on the Jacobian or on the Kummer surface as in Definition (3.5), but instead for Kummer coordinates as in Definition 2.8.

Definition 3.22. Let $x \in K_{\mathbb{A}}(k_v)$ be a set of Kummer coordinates on K. The *naive local height of x* is the quantity

$$\lambda_v(x) := -\frac{N_v}{n_v} v(x)$$

and the *canonical local height of x* is given by

$$\hat{\lambda}_v(x) := -\frac{N_v}{n_v}(v(x) + \mu_v(x)).$$

Notice that if k is a number field or function field of dimension 1 and $P \in J(k)$ is a point lying on a Jacobian surface J defined over k, then we have

$$h(P) = \frac{1}{d_k} \sum_{v \in M_k} n_v \lambda_v(x)$$

and

$$\hat{h}(P) = \frac{1}{d_k} \sum_{v \in M_k} n_v \hat{\lambda}_v(x)$$

for any choice x of Kummer coordinates for P because of the product formula (1.1). However, our function $\hat{\lambda}_v$ now depends on the choice of Kummer coordinates and not on the choice of a divisor in the class $[D_1]$. As in the case of elliptic curves, the canonical local height $\hat{\lambda}_v$ constructed as above has somewhat nicer properties than the canonical local height defined in Definition (3.5). Compare the following proposition, first stated and proved in [95], to (1.2).

Proposition 3.23. *(Stoll) Let $x, y, z, w \in K_{\mathbb{A}}(k_v)$. Then the following hold:*

(i) $\hat{\lambda}_v(\delta(x)) = 4\hat{\lambda}_v(x)$.

(ii) *If $w * z = B(x, y)$, then $\hat{\lambda}_v(z) + \hat{\lambda}_v(w) = 2\hat{\lambda}_v(x) + 2\hat{\lambda}_v(y)$.*

(iii) $\hat{\lambda}_v(x) = -\frac{N_v}{n_v} \lim_{n \to \infty} 4^{-n} v(\delta^{\circ n}(x))$.

(iv) *If k'/k_v is a finite extension, and v' is the extension of v to k', then we have $\hat{\lambda}_{v'}(x) = \hat{\lambda}_v(x)$.*

Proof. The validity of (i) can be shown using a straightforward computation:

$$\begin{aligned}\frac{n_v}{N_v}\hat{\lambda}_v(\delta(x)) &= -v(\delta(x)) - \sum_{n=0}^{\infty}\frac{1}{4^{n+1}}\varepsilon_v(\delta^{\circ(n+1)}(x)) \\ &= -4v(x) - \varepsilon_v(x) - \sum_{n=1}^{\infty}\frac{1}{4^n}\varepsilon_v(\delta^{\circ n}(x)) \\ &= 4\frac{n_v}{N_v}\hat{\lambda}_v(x).\end{aligned}$$

Property (ii) is also not hard to verify using Lemma 3.20 and Corollary 3.21:

$$\begin{aligned}&\frac{n_v}{N_v}\left(\hat{\lambda}_v(z)+\hat{\lambda}_v(w)\right) \\ &\quad= -v(w)-v(z)-\sum_{n=0}^{\infty}\frac{1}{4^{n+1}}\left(\varepsilon_v(\delta^{\circ n}(w))+\varepsilon_v(\delta^{\circ n}(z))\right) \\ &\quad= -v(B(x,y))+\varepsilon_v(x,y)-2\sum_{n=0}^{\infty}\frac{1}{4^{n+1}}\left(\varepsilon_v(\delta^{\circ n}(x))+\varepsilon_v(\delta^{\circ n}(y))\right) \\ &\quad= -2\left(v(x)+v(y)+\sum_{n=0}^{\infty}\frac{1}{4^{n+1}}(\varepsilon_v(\delta^{\circ n}(x))+\varepsilon_v(\delta^{\circ n}(y)))\right) \\ &\quad= 2\frac{n_v}{N_v}\left(\hat{\lambda}_v(x)+\hat{\lambda}_v(y)\right).\end{aligned}$$

(iii) follows from the fact that $\mu_v(x)$ is a bounded function, implying

$$\hat{\lambda}_v(\delta^{\circ n}(x)) = -\frac{N_v}{n_v}v(\delta^{\circ n}(x)) + \mathcal{O}(1),$$

combined with property (i).

Part (iv) is obvious from the definition of $\hat{\lambda}_v$. □

The canonical local height on Kummer coordinates also behaves well under isogenies. Compare the following to Proposition 2.5.

Proposition 3.24. *Let $\alpha : J \to J'$ be an isogeny of Jacobians of dimension 2 defined over k_v and let $d = \deg(\alpha)$. Then α induces a map $\alpha : K \to K'$ between the corresponding Kummer surfaces. We also get a well-defined induced map $\alpha : K_{\mathbb{A}} \longrightarrow K'_{\mathbb{A}}$ if we fix $a \in k_v^*$ and require $\alpha(0,0,0,1) = a(0,0,0,1)$. Moreover, we have*

$$\hat{\lambda}_v(\alpha(x)) = d\hat{\lambda}_v(x) + \log|a|_v$$

for any $x \in K_{\mathbb{A}}(k_v)$.

Proof. All assertions except for the last one are trivial. Using part (iii) of Proposition 3.23 it is enough to show

$$v(\delta^{\circ n}(\alpha(x))) = dv(\delta^{\circ n}(x)) - 4^n v(a) + \mathcal{O}(1).$$

However, we have $v(\alpha(x)) - dv(x) = \mathcal{O}(1)$ by assumption, so it suffices to show

$$v(\delta^{\circ n}(\alpha(x))) = v(\alpha(\delta^{\circ n}(x))) - (4^n - 1)v(a). \tag{3.15}$$

But since $\alpha : J \longrightarrow J'$ is an isogeny, it is a group homomorphism, so $\delta^{\circ n}(\alpha(x))$ and $\alpha(\delta^{\circ n}(x))$ represent the same point on K', hence they are projectively equal. Because they also have the same degree, the factor of proportionality is independent of x. We may therefore check (3.15) for a single x, so we take $x = (0,0,0,1) \in K_{\mathbb{A}}(k_v)$. Because we have $\delta(x) = x$ and, by assumption, $\alpha(x) = ax'$, where $x' = (0,0,0,1)$, we find

$$\delta^{\circ n}(\alpha(x)) = a^{4^n} x' \text{ and } \alpha(\delta^{\circ n}(x)) = ax',$$

thereby proving (3.15) and hence the proposition. □

The preceding proposition is particularly useful in order to analyze the behavior of the canonical local height under a change of model, which we also call a *transformation*, of the curve. Any such transformation τ is given by data $([a,b,c,d], e, U)$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(k_v), e \in k_v^*$ and $U(X,Z) \in k_v[X,Z]$ is homogeneous of degree 3. If we apply such a transformation $\tau = ([a,b,c,d], e, U)$ to an affine point (ξ, η) on the curve, then we get

$$\tau(\xi,\eta) = \left(\frac{a\xi + b}{c\xi + d}, \frac{e\eta + U(\xi,1)}{(c\xi+d)^3} \right). \tag{3.16}$$

A transformation also acts on the forms F and H by

$$\begin{aligned} \tau^* F(X,Z) &= (ad-bc)^{-6} \left(e^2 F' + (eH' - U')U' \right) \\ \tau^* H(X,Z) &= (ad-bc)^{-3} \left(eH' - 2U' \right), \end{aligned}$$

where

$$S' = S(dX - bZ, -cX + aZ)$$

for any binary form $S(X,Z) \in k_v[X,Z]$.

The map which a transformation $\tau = ([a,b,c,d], e, U)$ induces on $K_{\mathbb{A}}$ will play a crucial part later on. Therefore we give it here explicitly. Let $x = (x_1, x_2, x_3, x_4) \in K_{\mathbb{A}}$ and let

$$U(X,Z) = u_0 Z^3 + u_1 XZ^2 + u_2 X^2 Z + u_3 X^3.$$

Then $\tau(x)$ is equal to the following quadruple, where we have fixed the constant factor to be $(ad-bc)^{-1}$:

$$\begin{aligned}(ad-bc)^{-1}\Big(&d^2x_1+cdx_2+c^2x_3,\\ &2bdx_1+(ad+bc)x_2+2acx_3,\\ &b^2x_1+abx_2+a^2x_3,\\ &(ad-bc)^{-2}(e^2x_4+(l_{1,1}+l_{1,2}+l_{1,3})x_1+(l_{2,1}+l_{2,2}+l_{2,3})x_2\\ &+(l_{3,1}+l_{3,2}+l_{3,3})x_3)\Big),\end{aligned}$$

where for $i=1,2,3$ we have

$$\begin{aligned}l_{i,1}&=\frac{e^2}{(ad-bc)^4}l'_{i,1} \text{ with } l'_{i,1}\in\mathbb{Z}[f_0,\dots,f_6,a,b,c,d],\\ l_{i,2}&=\frac{e}{(ad-bc)^4}l'_{i,2} \text{ with } l'_{i,2}\in\mathbb{Z}[h_0,\dots,h_3,u_0,\dots,u_3,a,b,c,d],\\ l_{i,3}&=\frac{1}{(ad-bc)^4}l'_{i,3} \text{ with } l'_{i,3}\in\mathbb{Z}[u_0,\dots,u_3,a,b,c,d].\end{aligned}$$

All of the $l'_{i,j}$ are homogeneous of degree 8 in a,b,c,d and are homogeneous in the other variables. More precisely, the $l'_{i,1}$ are linear in the f_j, the $l'_{i,2}$ are linear in the u_j and also linear in the h_l, whereas the $l'_{i,3}$ are quadratic in the u_j. So we see that τ acts on k_v^4 as a linear map whose determinant has valuation $v(\tau)=2v(e)-3v(ad-bc)$. The following corollary was first proved as [95, Proposition 3.2]; in fact we generalized the proof given there in order to prove our Proposition 3.24.

Corollary 3.25. *Let $\tau=([a,b,c,d],e,U)$ be a change of model of a genus 2 curve C with associated Kummer surface K. Then we have*

$$\hat{\lambda}_v(\tau(x))=\hat{\lambda}_v(x)-\frac{N_v}{n_v}v(\tau).$$

for any $x\in K_{\mathbb{A}}(k_v)$

Definition 3.26. Let C be a genus 2 curve over k_v given by a model (3.13) with discriminant $\Delta(C)$ and let K be the associated Kummer surface. We call the function

$$\begin{aligned}\tilde{\lambda}_v: K_{\mathbb{A}}(k_v) &\longrightarrow \mathbb{R}\\ x &\mapsto \hat{\lambda}_v(x)-\frac{1}{10}\log|\Delta(C)|_v\end{aligned}$$

the *normalized canonical local height on $K_{\mathbb{A}}(k_v)$*.

Corollary 3.27. *The normalized canonical local height is independent of the given model of C.*

Proof. Let τ be a change of model. Then we have

$$v(\Delta(\tau(C))) = v(\Delta(C)) + 10v(\tau).$$

□

Recall that for simplified models (that is models of the form $Y^2 = F(X,1)$) we defined four divisors

$$D_i = \{P \in J : \kappa_i(P) = 0\} \subset \mathrm{Div}(J)(k_v),$$

see (3.5), where in particular $D_1 = 2\Theta$ or $D_1 = \Theta^+ + \Theta^-$, according to whether C has a unique rational point at infinity or not. We extend this definition to the general case in the obvious way.

Let $P \in J(k_v) \setminus \mathrm{supp}(D_i)$ and let $x = (x_1, x_2, x_3, x_4)$ be a set of Kummer coordinates of P normalized by

$$x_j = \frac{\kappa_j(P)}{\kappa_i(P)}, \quad j \in \{1,2,3,4\}.$$

We proved that

$$\lambda_{i,v}(P) := \lambda_v(x)$$

is a Weil function and

$$\hat{\lambda}_{i,v}(P) := \hat{\lambda}_v(x)$$

is the canonical local height on J associated with D_i, v and $g_i(P) = \delta_i(x)$ in the simplified case $H = 0$. Both the definitions and the proofs carry over to the general case.

3.4.2 The "kernel" of ε_v revisited

We want to generalize Theorem 3.9, stating that if v is non-archimedean and $H = 0$, then

$$U_v := \{P \in J(k_v) : \varepsilon_v(P) = 0\}$$

is a subgroup of $J(k_v)$, to the general case.

The proof of Theorem 3.9 presented in [94, §4] relies heavily on [94, Proposition 3.1]. We want to generalize that proof and so we first generalize [94, Proposition 3.1].

Let l be a field of characteristic 2; let $C_{F,H}$ be a curve in weighted projective space with respective weights 1, 3, 1 assigned to the variables X, Y, Z that is given by an equation

$$Y^2 + H(X,Z)Y = F(X,Z),$$

where

$$F(X,Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

and

$$H(X,Z) = h_0Z^3 + h_1XZ^2 + h_2X^2Z + h_3X^3$$

are binary forms in $l[X,Z]$ of respective degrees 6 and 3. Let $K_{F,H}$ denote the subscheme of $\mathbb{P}^3$ given by the vanishing of (3.11) as in Lemma 3.13. Then the constructions of the objects $\delta = (\delta_1, \ldots, \delta_4)$ and B_{ij} still make sense in this context, but we may now have $\delta_i(x) = 0$ for all $1 \leq i \leq 4$ (which we abbreviate by $\delta(x) = 0$) or $B_{ij}(x,y) = 0$ for all $1 \leq i,j \leq 4$ (which we abbreviate by $B(x,y) = 0$) for sets x, y of Kummer coordinates on $K_{F,H}$. Proposition [94, 3.1] says more about these phenomena in the classical case $\operatorname{char} l \neq 2$, $H = 0$.

Lemma 3.28. *Let $x, y \in K_{F,H}(l)$.*

(1) If $\delta(\delta(x)) = 0$, then we already have $\delta(x) = 0$.

(2) If $B(x,y) = 0$, then we must have $\delta(x) = \delta(y) = 0$.

Proof. We may assume without loss of generality that l is algebraically closed. If the given curve is smooth, then the result is obvious, because the situations described in the statement can never occur. If it is not smooth, note that since we can act on F and H using transformations of the form (3.16), it is enough to consider only one representative of each orbit under such transformations. This is similar to the strategy in the proof of [94, Proposition 3.2], except that we now have two forms to deal with, but also a larger group of transformations acting on them. We can, for example, pick the following representatives:

(i) $H = 0, \quad F = 0,$

(ii) $H = Z^3, \quad F = 0,$

(iii) $H = Z^3, \quad F = aXZ^5, \quad a \neq 0,$

(iv) $H = XZ^2, \quad F = aXZ^5, \quad a \neq 0,$

(v) $H = XZ^2, \quad F = bXZ^3, \quad b \neq 0,$

(vi) $H = Z^3, \quad F = aXZ^5 + bX^3Z^3, \quad b \neq 0,$

(vii) $H = XZ^2, \quad F = 0,$

(viii) $H = X^2Z + XZ^2, \quad F = bX^3Z^3, \quad b(b+1) = 0,$

(ix) $H = X^2Z + XZ^2, \quad F = bX^3Z^3, \quad b(b+1) \neq 0,$

(x) $H = X^2Z + XZ^2, \quad F = aXZ^5 + bX^3Z^3, \quad a(a^2 + a + b + b^2) \neq 0,$

(xi) $H = XZ^2, \quad F = aXZ^5 + bX^3Z^3, \quad ab \neq 0,$

(xii) $H = 0, \quad F = XZ^5,$

(xiii) $H = 0, \quad F = X^3Z^3.$

We prove the statement of the Proposition for each representative using elementary methods similar to the proof of [94, Proposition 3.1] in Appendix A.3. □

Using Lemma 3.28 we can show:

Theorem 3.29. *Suppose that v is non-archimedean and that J is a Jacobian surface over k_v. Let $U_v := \{P \in J(k_v) : \varepsilon_v(P) = 0\}$. Then U_v is a subgroup of finite index in $J(k_v)$ and ε_v factors through the quotient $J(k_v)/U_v$. Moreover we have that $\varepsilon_v(-P) = \varepsilon_v(P)$ and U_v contains the kernel of reduction with respect to the given model.*

Proof. If $\mathrm{char}(\mathfrak{k}_v) \neq 2$, then we can use the usual isomorphism $\tau : (x, y) \mapsto (x, 2y + H(x, 1))$ and Theorem 3.9.

So suppose that $v(2) > 0$. The theorem follows from Corollary 3.21 and Lemma 3.28 exactly as in the proof of Theorem 3.9 given in [94, §4].

□

3.4.3 Relation to Néron models

In the case of elliptic curves a crucial point in the determination of explicit formulas for the function μ_v in case of non-archimedean v is the fact that ε_v and μ_v factor through the group of components Φ_v of the Néron model whenever the given model is v-minimal, see Proposition 2.14 and Remark 2.15. This basically follows from Lemma 2.12, stating that the given Weierstrass equation is v-minimal if and only if it is geometrically minimal, that is, if the minimal proper regular model is a desingularization of the closure of the Weierstrass model.

In the present situation it is unfortunately not true any longer that v-minimality of the given model is sufficient for ε_v and μ_v to factor through Φ_v and we will see examples of this phenomenon later on. Instead, recall from Remark 2.13 that another criterion for v-minimality of Weierstrass models is that their closures have rational singularities. This turns out to be the correct condition for a suitable analog of Proposition 2.14.

Recall the definitions and results from Section 1.5, in particular the definition of proper regular models and the results on the relative Picard functor.

Theorem 3.30. *Let C be a smooth projective geometrically connected curve of genus 2, given by a model of the form (3.13), whose closure $\mathcal{C}$ over $\operatorname{Spec}(\mathcal{O}_v)$ is normal and flat and has rational singularities. Then ε_v and μ_v factor through the component group Φ_v of the Néron model of the Jacobian J of C.*

Proof. Because of Theorem 3.29 it suffices to show that ε_v vanishes for points lying in $J_0(k_v)$, where $J_0(k_v)$ is the set of points of $J(k_v)$ mapping to $\mathcal{J}_v^0(\mathfrak{k}_v)$. If $P \in J(k_v)$, then we denote by $x(P)$ a set of v-integral Kummer coordinates such that one of the entries has valuation equal to 0.

First note that C must satisfy condition (†), since it is of genus 2. One easy way to check this is to look at the classification [76] of Namikawa-Ueno. Indeed, every possible minimal proper regular model of a genus 2 curve has a component of simple multiplicity. Hence we have an interpretation of the identity component $\mathcal{J}^0$ (the scheme with generic fiber $\mathcal{J}_{k_v}$ and special fiber $\mathcal{J}_v^0$) in terms of data on the curve; namely, Proposition 1.36 says that we have an isomorphism

$$\mathcal{J}^0 \cong \operatorname{Pic}^0_{\mathcal{C}/\operatorname{Spec}(\mathcal{O}_v)}, \tag{3.17}$$

where the latter is the identity component of the relative Picard functor $\operatorname{Pic}_{\mathcal{C}/\operatorname{Spec}(\mathcal{O}_v)}$, which in this case can be represented by a separated scheme.

Let $P' \in \mathcal{J}_v^0(\mathfrak{k}_v)$ be of the form $P' = \sigma_P(v)$, where $P \in J_0(k_v)$ and $\sigma_P : \operatorname{Spec}(\mathcal{O}_v) \longrightarrow \mathcal{J}$ denotes the section associated to P. Then P' lies in the support of the closure $D_{i,\mathcal{J}}$ of D_i on $\mathcal{J}$ if and only if $v(x(P)_i) > 0$, or, put differently, if the reduction of $x(P)_i$ vanishes, because of the isomorphism (3.17). Here we have to remember multiplicities when taking the closure, see the discussion following (1.3).

But this means that if $v(x_j(P)) = 0$ for some $j \in \{1,2,3,4\}$, then $D_{i,\mathcal{J}}$ is represented by $\frac{\kappa_i(P)}{\kappa_j(P)}$ around P. Therefore (1.4) implies that we have

$$i(D_i, P) = v\left(\frac{\kappa_i(P)}{\kappa_j(P)}\right).$$

We first consider $i = 4$. By Theorem 1.17 we obtain

$$\hat{\lambda}_{4,v}(P) = \frac{N_v}{n_v}(i(D_4, P) + \gamma_0(D_4))$$

for any point $P \in J_0(k_v) \setminus \operatorname{supp} D_4$.

But the image of the origin on the Kummer surface is represented in normalized form by $x = x(O) = (0,0,0,1)$, it certainly maps to $\mathcal{J}_v^0$ and furthermore we have $\lambda_v(x) = 0 = v(x)$. Because we also have $\hat{\lambda}_v(x) = \hat{\lambda}_{4,v}(x)$, we deduce

$$\gamma_0(D_4) = \frac{n_v}{N_v}\hat{\lambda}_{4,v}(0) - i(D_4, 0) = 0,$$

as $i(D_4, O) = 0$.

Since the Néron model does not change under unramified extensions of the ground field, we can make such an extension for each $i < 4$ to ensure that we have some $P \in J_0(k_v)$ such that we can find a set of Kummer coordinates $x = x(P) = (x_1, x_2, x_3, x_4)$ for P that satisfies $v(x_i(P)) = v(x_4(P)) = 0$. Then

$$\hat{\lambda}_v(x) = \hat{\lambda}_{4,v}(P) = \frac{N_v}{n_v}(i(D_4, P) + \gamma_0(D_4)) = 0,$$

but on the other hand we see

$$\hat{\lambda}_v(x) = \hat{\lambda}_{i,v}(P) = \frac{N_v}{n_v}(i(D_i, P) + \gamma_0(D_i)) = \frac{N_v}{n_v}\gamma_0(D_i);$$

thus $\gamma_0(D_i) = 0$ follows for all i.

For any $P \in J_0(k_v)$ we can find some $i \in \{1, 2, 3, 4\}$ satisfying $v(x_i) = 0$, where $x = x(P)$. Therefore we find

$$\hat{\lambda}_v(x) = \hat{\lambda}_{i,v}(P) = \frac{N_v}{n_v}(i(D_i, P) + \gamma_0(D_i)) = 0,$$

but also

$$\hat{\lambda}_v(x) = -\frac{N_v}{n_v}(v(x) + \mu_v(P)) = -\frac{N_v}{n_v}\mu_v(P),$$

hence $\mu_v(P) = 0$ and $\varepsilon_v(P) = 0$ follow for any $P \in J_0(k_v)$. □

Remark 3.31. Liu has extended the theory of v-minimal Weierstrass models to arbitrary hyperelliptic curves, see [63]. In fact he proves, in analogy with elliptic curves, that if the given model of the form (3.13) is v-minimal and there is an $\mathcal{O}_v$-rational point on C, then the given model is geometrically minimal (see [63, Corollaire 5]).

See Example 3.61 for a genus 2 curve given by geometrically minimal models whose closure over $\mathrm{Spec}(\mathcal{O}_v)$ does not have rational singularities, where ε_v and μ_v do not factor through Φ_v. In fact this already holds for the curve from Example 1.33, continued in Example 3.68.

Recall that apart from the computation of canonical heights we are also interested in finding upper bounds for

$$\beta_v = \sup\{|\mu_v(P)| : P \in J(k_v)\}.$$

In some situations, we can use Theorem 3.30 for this purpose.

Corollary 3.32. *Suppose that the given model of C satisfies the hypotheses of Theorem 3.30. Also suppose that the Tamagawa number $c_v = \#\Phi_v(\mathfrak{k}_v)$ is at most 3 and that, in case $c_v > 1$, we have computed $\varepsilon_v(P) \neq 0$ for some $P \in J(k_v)$.*

(i) *If $c_v = 1$, then $\beta_v = 0$.*

(ii) *If* $c_v = 2$, *then* $\beta_v = \frac{\varepsilon_v(P)}{4}$.

(iii) *If* $c_v = 3$, *then* $\beta_v = \frac{\varepsilon_v(P)}{3}$.

Remark 3.33. We may have $c_v \leq 3$ even when $\#\Phi_v$ is much larger. We can compute c_v using [10, Theorem 1.17]; see also the discussion in [44, §3.4]. This is especially useful when we have $\#\Phi_v > 3$, but suspect that $c_v < 4$. Another possible application is the situation where we have $\#\Phi_v = 3$, but no point $P \in J(k_v)$ of small naive height satisfies $\varepsilon_v(P) \neq 0$. Here it is sometimes possible to show $c_v = 1$ and thus $\beta_v = 0$.

Remark 3.34. Often we can even improve the bounds obtained by checking all v-adic points on the Kummer surface, because such a search will usually only be an optimal bound γ_v on $|\varepsilon_v|$ and not on $|\mu_v|$. If, for example, we know that the closure of our model has rational singularities and $\#\Phi_v = 2$, then we can improve the bound $\gamma_v/3$ to $\gamma_v/4$. When the residue characteristic is large, even this tiny improvement can make a difference, because improvements in the bound on the height constant show up exponentially in the computation of generators of the Mordell-Weil group.

3.4.4 Simplifying the model

We continue to consider non-archimedean v and let $\pi = \pi_v$ denote a uniformiser. In the case of elliptic curves it is possible to find explicit formulas for μ_v depending on the reduction type of the minimal proper regular model of the curve over $\mathrm{Spec}(\mathcal{O}_v)$ in all cases. This relies on two observations:

1. There are essentially only ten different reduction types and they are well understood and easily distinguishable using Tate's algorithm.

2. Each elliptic curve has a model such that ε_v and μ_v factor through Φ_v.

In contrast to this, there are more than 100 different reduction types for minimal proper regular models of genus 2 curves, classified in [76] and there are curves that have no model satisfying the hypotheses of Theorem 3.30, that is, having rational singularities. Therefore we must look for simplifications.

Because the canonical local height $\hat{\lambda}_v$ behaves so nicely under isogenies, in particular under isomorphisms induced by transformations of the underlying curve, we can simplify the computation of the canonical local height significantly as follows. The idea is to apply transformations until either $\varepsilon_v(P)$ becomes trivial or we cannot simplify the model any further. We show that in the latter case we always end up in one of five different situations and we prove simple formulas for $\mu_v(P)$ or for $\mu_v(nP)$, where n is small – we always have $n \leq 4$ except for one rather exotic reduction type.

If necessary, we first apply a transformation to make sure that the reduction of C is reduced. This is easy, if we allow field extensions of ramification

index 2, see the proof of Proposition 3.36 below. We may do so because of part (iv) of Proposition 3.23, telling us that the canonical local height is invariant under extensions.

However, we must first discuss how one can define and compute the multiplicity of a point P lying on the reduction of C.

Definition 3.35. Let l be a field and let $C_{F,H}$ be a reduced curve in weighted projective space with respective weights 1, 3, 1 assigned to the variables X, Y, Z that is given by an equation

$$Y^2 + H(X,Z)Y = F(X,Z),$$

where $F, H \in l[X,Z]$ are homogeneous of degrees 6 and 3, respectively. The *multiplicity* $\delta(P, C_{F,H})$ *of* $P = (X_0 : Y_0 : Z_0) \in C_{F,H}$ is defined as follows:

- If P is a singular point of type A_n, then $\delta(P, C_{F,H}) = n + 1$.
- If P is fixed by the involution $(X : Y : Z) \mapsto (X : Y - H(X,Z) : Z)$, then $\delta(P, C_{F,H}) = 1$.
- Otherwise $\delta(P, C_{F,H}) = 0$.

We say that P is a *node of* $C_{F,H}$ if $\delta(P, C_{F,H}) = 2$ and we call P a *cusp of* $C_{F,H}$ if $\delta(P, C_{F,H}) = 3$. If $S(X,Z)$ is any binary form, then we also define $\delta(P,S)$ to be n if we can write

$$S(X,Z) = (Z_0X - X_0Z)^n S'(X,Z),$$

where $S'(X_0, Z_0) \neq 0$.

If the characteristic of l is not equal to 2, then it is easy to compute the multiplicity. Namely, we have

$$\delta(P, C_{F,H}) = \delta(\tau(P), 4F(X,Z) + H(X,Z)^2),$$

where

$$\tau((X : Y : Z)) = (X : 2Y + H(X,Z) : Z).$$

In particular, if $H = 0$, then the multiplicity of $P = (X_0 : Y_0 : Z_0)$ is simply the multiplicity of $(Z_0X - X_0Z)$ in F.

If the residue characteristic is 2, we can use a method due to Liu to compute the multiplicity $\delta(P, C_{F,H})$. So suppose we are in this situation.

If $P = (X_0 : Y_0 : Z_0) \in C_{F,H}$, then we see that P must be nonsingular and hence $\delta(P, C_{F,H}) \leq 1$ unless $H(X_0, Z_0) = 0$. So we assume that the latter holds and let $G(X,Z)$ denote the linear form dividing H and satisfying $G(X_0, Z_0) = 0$. For any binary form $S(X,Z)$ we write $\delta(P,S)$ for the multiplicity of G in S.

If we have $2\delta(P,H) \leq \delta(P,F)$ or if $\delta(P,F)$ is odd, then we get

$$\delta(P, C_{F,H}) = \min\{2\delta(P,H), \delta(P,F)\}. \tag{3.18}$$

Otherwise, let $2n = \delta(P,F)$ and write

$$F(X,Z) = \sum_{i \geq 2n} D_i(X,Z)G(X,Z)^i.$$

There is some $U(X,Z) \in l[X,Z]$ such that $G(X,Z)$ divides $U(X,Z)^2 - D_{2n}(X,Z)$. We change our equation using the transformation $\tau : Y \mapsto Y + U(X,Z)G(X,Z)^n$. Then we have $\delta(\tau(P), \tau(C_{F,H})) = \delta(P, C_{F,H})$ and $\delta(\tau(P), \tau^* H) = \delta(P,H)$; however, it is clear that

$$\delta(\tau(P), \tau^* F) > \delta(P,F) \tag{3.19}$$

holds. Hence we can read off the multiplicity $\delta(P, C_{F,H})$ after applying a finite number of these steps.

This method works for the computation of the multiplicity of a point lying on a reduced curve defined by an equation of the form

$$C_{F,H} : Y^2 + H(X,Z)Y = F(X,Z),$$

in weighted projective space $\mathbb{P}^2_l(1, g+1, 1)$, where we have $g \geq 1$ and $H(X,Z), F(X,Z) \in l[X,Z]$ are binary forms of degrees $g+1$ and $2g+2$, respectively, defined over a field l of characteristic 2.

We assume that l is algebraically closed and that $\mathrm{char}(l) = 2$, for the moment. As in the case $\mathrm{char}(l) \neq 2$, the multiplicity does not change if we act on $C_{F,H}$ by a transformation of the form (3.16). Recall the list of representatives (i)–(xiii) for each orbit under the action induced by transformations of the form (3.16) given in the proof of Lemma 3.28.

Table 3.2 contains the following information, in parts retrieved from Appendix A.3: For each representative we have listed for a point $x = (x_1 : x_2 : x_3 : x_4) \in K$ the condition (cond.) that must be satisfied in order for all $\delta_i(x)$ to vanish. Moreover, we have listed under (add.) the condition, if any, that a point $x = (x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3$ satisfying (cond.) must satisfy in order to lie on K. Finally we have listed the multiplicities (mults.) that the curve defined by (3.13) has at the points $(X : Z) = (1 : 0)$, $(X : Z) = (0 : 1)$ and $(X : Z) = (1 : 1)$, in case the multiplicities there are greater than 1. For example, for type (vii) the entry is $(4, 2)$, which means that it has multiplicity 4 at $(1 : 0 : 0)$ and multiplicity 2 at $(0 : 0 : 1)$.

Now let us return to our original setup of a genus 2 curve defined over k_v, where $v \in M_k^0$. We want to show that we can always reduce to a

Type	cond.	add.	mults.
(i)	$x_4 = 0$		
(ii)	$x_4 = 0$		(6)
(iii)	$x_4 = 0$	$x_1 = 0$	(5)
(iv)	$x_4 = 0$	$x_1 = 0$	(4)
(v)	$x_4 = 0$	$x_1x_3 = 0$	(3,2)
(vi)	$x_1 = x_4 = 0$		(3)
(vii)	$x_4 = 0$		(4,2)
(viii)	$x_4 = 0$		(2,2,2)
(ix)	$x_4 = 0$	$x_1x_3 = 0$	(2,2)
(x)	$x_1 = x_4 = 0$		(2)
(xi)	$x_1 = x_4 = 0$		(3)
(xii)	$x_4 = 0$		(5)
(xiii)	$x_4 = 0$	$x_1x_3 = 0$	(3,3)

Table 3.2: Conditions for the vanishing of $\delta(x)$ and multiplicities of C

small number of cases for which we can find simple formulas to compute the canonical local height and then use Corollary 3.25 to find the canonical local height of our original point. The drawback of this approach is that we might have to extend the ground field and this extension may be ramified. However, the next proposition asserts that at least the primes dividing the ramification index are small and typically the ramification index itself is as well. It is taken from [95] where it was proved for residue characteristic not equal to 2; the proof remains the same in the general case.

Proposition 3.36. *(Stoll) There is an extension k'/k_v of ramification index not divisible by a prime $p > 5$ such that C has a model over k' of the form $Y^2 + H(X,1)Y = F(X,1)$ whose special fiber has no point of multiplicity greater than three and at most one point of multiplicity exactly three. Here multiplicity means multiplicity on the special fiber, introduced in Definition 3.35.*

Proof. If the given model of C is not reduced, we can transform it until we have $\tilde{H} = \tilde{F} = 0$. Now we simply scale Y by a suitable power of π; we may be required to use a ramified field extension of degree 2 in order to do this.

Hence we may assume that at least one of $\tilde{F}$ and $\tilde{H}$ does not vanish. There are exactly six ramification points of C over $\mathbb{P}^1_{k_v}$, namely the Weierstrass points of C. They reduce to six points, counted with multiplicity, on $\mathbb{P}^1_{\mathfrak{k}_v}$, which we view as the special fiber of a model of $\mathbb{P}^1$ over $\mathrm{Spec}(\mathcal{O}_v)$. Whenever several ramification points reduce to the same point on this special fiber, then we can blow up that point. Repeated application of this yields another model W of $\mathbb{P}^1$ over $\mathrm{Spec}(\mathcal{O}_v)$ such that the ramification points of C map to distinct points on the special fiber W_v of W.

If necessary, we can contract components of W_v in order to get a unique model W' such that the last condition still holds, but we also have the property that every component of the special fiber of W' of self-intersection -1 contains the image of at least 2 of the ramification points. For combinatorial reasons it is always possible to pick one component such that after contracting all other components we get a model W'' of $\mathbb{P}^1$ whose special fiber consists of a single component and such that at most three ramification points map to the same point on this special fiber, and this can happen at most once.

However, the generic fiber of W'' may not be defined over k_v. Hence we have to analyze the ramification index of the smallest extension k'/k_v such that W'' is defined over the spectrum of the ring of integers of k'. This will also provide us with a more explicit description of the process outlined above.

We try to minimise the valuation of the discriminant of the model of C while allowing ramified field extensions with some restriction on the ramification index. Suppose we have a point, say at $(0:0:1)$, on the reduction $\tilde{C}$ of C of multiplicity $n \geq 3$. We can find the largest $d > 0$, where $d \in \mathbb{Q}$ is not necessarily integral, such that both $\pi^{-d}F(\pi^{d/n}X, Z)$ and $\pi^{-d}H(\pi^{d/n}X, Z)$ are integral over the ring of integers of a suitable field extension of ramification index e, where e is the least common multiple of the denominators of d and $\frac{d}{n}$, written as quotients of coprime integers. Obviously e cannot be divisible by a prime other than 2, 3 or 5. Let τ denote the transformation corresponding to this; then an application of τ corresponds to moving from one component of W'_v to another.

The effect of the transformation τ on the discriminant $\Delta(C)$ is given by

$$v(\Delta(\tau(C))) = v(\Delta(C)) - 10d\left(1 - \frac{3}{n}\right).$$

In case $n \geq 4$ the transformation τ thus reduces the valuation of the discriminant and hence iterating this process leads to a model whose points all have multiplicity < 4 in a finite number of steps. If we have $n = 3$ and $\tilde{C}$ has another point Q of multiplicity 3, then τ keeps the valuation of the discriminant constant and does not change the multiplicity of Q, but the selected singularity may split up into several points of lower multiplicity. If it does not, we iterate the process; the selected singularity must split up after a finite number of steps. □

Remark 3.37. Suppose that $n \geq 4$ in the notation of the above proof. If $v(2) = 0$, then we can assume $H = 0$ and the effect of τ on the Newton polygon of F indicates that the only way we can have a root of multiplicity n after applying τ is if the roots are very close v-adically. In general, the number of steps depends on how close the ramification points are v-

adically, since extending the field as above corresponds to "zooming in" on the ramification points.

If $n = 3$, then considering the Newton polygon of $\tilde{F}$ in case $v(2) = 0$ and $H = 0$ also shows why the method outlined in the proof of Proposition 3.36 only works if there are two points of multiplicity 3.

Now we distinguish between $\mathrm{char}(\mathfrak{k}_v) \neq 2$ and $\mathrm{char}(\mathfrak{k}_v) = 2$. If the residue characteristic is not 2, then we can apply a transformation to ensure $H = 0$. Proposition 3.36 says that over a suitable extension of k_v the reduction of F has no root of multiplicity greater than 3 and at most one root of exact multiplicity 3. This means that we can assume, using Table 3.1, that, possibly after making an unramified field extension, the reduction of F belongs to one of the five cases given below. We leave out the case of square-free reduction, because then ε_v is trivial. Let $x = (x_1, x_2, x_3, x_4)$ denote a set of integral Kummer coordinates for P such that one of the entries is a unit and let $\tilde{x} = (\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{x}_4)$ be its reduction.

(1) $\tilde{F} = X(X - Z)(X - aZ)(X - bZ)Z^2, \quad a \neq b, \quad a, b \neq 0, 1, \quad \tilde{x}_1 = \tilde{x}_4 = 0.$

(2) $\tilde{F} = X^2(X - Z)(X - aZ)Z^2, \quad a \neq 0, 1, \quad \tilde{x}_1\tilde{x}_3 = \tilde{x}_4 = 0.$

(3) $\tilde{F} = X^2(X - Z)^2Z^2, \quad \tilde{x}_4 = 0.$

(4) $\tilde{F} = X^3(X - Z)(X - aZ)Z, \quad a \neq 0, 1, \quad \tilde{x}_3 = \tilde{x}_4 = 0.$

(5) $\tilde{F} = X^3(X - Z)Z^2, \quad \tilde{x}_1\tilde{x}_3 = \tilde{x}_4 = 0.$

In case the residue characteristic is 2, we look at Table 3.2 and find that we can always reduce to one of the following situations, possibly after an unramified extension of the base field.

(1) $\tilde{H} = X^2Z + XZ^2, \quad \tilde{F} = aXZ^5 + bX^3Z^3, \quad a(a^2 + a + b + b^2) \neq 0, \quad \tilde{x}_1 = \tilde{x}_4 = 0.$

(2) $\tilde{H} = X^2Z + XZ^2, \quad \tilde{F} = bX^3Z^3, \quad b(b + 1) \neq 0, \quad \tilde{x}_1\tilde{x}_3 = \tilde{x}_4 = 0.$

(3) $\tilde{H} = X^2Z + XZ^2, \quad \tilde{F} = bX^3Z^3, \quad b(b + 1) = 0, \quad \tilde{x}_4 = 0.$

(4) (i) $\tilde{H} = X^3, \quad \tilde{F} = bX^3Z^3 + aX^5Z, \quad b \neq 0, \quad \tilde{x}_3 = \tilde{x}_4 = 0.$
(ii) $\tilde{H} = X^2Z, \quad \tilde{F} = bX^3Z^3 + aX^5Z, \quad ab \neq 0, \quad \tilde{x}_3 = \tilde{x}_4 = 0.$

(5) $\tilde{H} = X^2Z, \quad \tilde{F} = bX^3Z^3, \quad b \neq 0, \quad \tilde{x}_1\tilde{x}_3 = \tilde{x}_4 = 0$.

Explicit formulas for all cases will be determined in Section 3.6. Note that for the sake of a consistent normalization, we always move the first node we encounter to ∞ and a cusp (unique by construction) to $(0 : 0 : 1)$.

3.5 Igusa invariants

In this section we discuss how we can distinguish between different types of reduction using certain invariants of genus 2 curves. These are classical objects that were introduced by Igusa in [55] in order to construct the moduli scheme of genus 2 curves up to isomorphism. It turns out that this is an affine scheme of dimension 3. More precisely, it is the spectrum of a ring that can be generated by 10 elements over $\mathbb{Z}$, see for instance [70] for an explicit set of generators.

Let l be a field of characteristic not equal to 2 and consider the invariants $J_2, J_4, J_6, J_8, J_{10}$ defined in [55], commonly called *Igusa invariants*. Then $J_{2i}(F)$ is an invariant of binary sextics of degree $2i$ and if

$$F(X,Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

is a binary sextic, then $J_{2i}(F) \in \mathbb{Z}[\frac{1}{2}, f_0, \ldots, f_6]$. In particular we have $J_{10}(F) = 2^{-12}\operatorname{disc}(F)$. It is shown in [55] that the invariants J_2, J_4, J_6, J_{10} generate the even degree part of the ring of invariants of binary sextics. Since the characteristic of l is not equal to 2 we can find a model of C of the form $Y^2 = F(X,1)$, where $F \in l[X,Z]$ is a binary sextic, so it makes sense that these invariants can be used in the theory of such curves. But it is rather surprising that they are also useful in case $\operatorname{char}(l) = 2$.

The following is taken essentially from [64]:

Definition 3.38. Let l be a field and consider the curve given by the equation

$$C_{F,H} : Y^2 + H(X,Z)Y = F(X,Z),$$

in weighted projective space $\mathbb{P}^2_l(1,3,1)$ with weights 1, 3 and 1 for the variables X, Y and Z, respectively, where $H(X,Z), F(X,Z) \in l[X,Z]$ are binary forms of degrees 3 and 6, respectively. If $\operatorname{char}(l) \neq 2$, we define the *Igusa invariants of* $C_{F,H}$ as

$$J_{2i}(C_{F,H}) := J_{2i}\left(4F(X,Z) + H(X,Z)^2\right).$$

If $\operatorname{char}(l) = 2$, then let $W(l)$ be the ring of Witt vectors of l and let $H'(X,Z), F'(X,Z) \in W(l)[X,Z]$ be lifts of H and F, respectively, to $W(l)$. We define the *Igusa invariants of* $C_{F,H}$ as

$$J_{2i}(C_{F,H}) := J_{2i}\left(4F'(X,Z) + H'(X,Z)^2\right) \pmod{2W(l)}.$$

We need to define two additional invariants, namely

$$I_4(C_{F,H}) := J_2(C_{F,H})^2 - 2^3 3 J_4(C_{F,H})$$

and

$$\begin{aligned} I_{12}(C_{F,H}) &:= -2^3 J_4(C_{F,H})^3 + 3^2 J_2(C_{F,H}) J_4(C_{F,H}) J_6(C_{F,H}) \\ &\quad -3^3 J_6(C_{F,H})^2 - J_2(C_{F,H})^2 J_8(C_{F,H}). \end{aligned}$$

Parts of the following theorem were proved by Igusa in [55], by Mestre in [70] and by Liu in [64]. Since no published proof of the entire result can be found in the literature (especially for the case of characteristic 2, where apparently nothing has been written down except for part (i) due to Liu), we provide a complete proof.

Theorem 3.39. *Let l be a field and let $C_{F,H}$ be the curve given by the equation*

$$Y^2 + H(X,Z)Y = F(X,Z),$$

in $\mathbb{P}^2_l(1,3,1)$ where $H(X,Z), F(X,Z) \in l[X,Z]$ are binary forms of degree 3 and 6, respectively. Let $J_{2i} := J_{2i}(C_{F,H})$ and $I_j := I_j(C_{F,H})$, where $i \in \{1,\ldots,5\}$ and $j \in \{4,12\}$.

(i) *$C_{F,H}$ is smooth $\iff$ $J_{10} \neq 0$.*

(ii) *$C_{F,H}$ has a unique node and no point of higher multiplicity $\iff$ $J_{10} = 0$ and $I_{12} \neq 0$.*

(iii) *$C_{F,H}$ has exactly two nodes $\iff$ $J_{10} = I_{12} = 0$ and $I_4 J_4 J_6 \neq 0$.*

(iv) *$C_{F,H}$ has three nodes $\iff$ $J_{10} = I_{12} = J_4 J_6 = 0$ and $I_4 \neq 0$.*

(v) *$C_{F,H}$ has a cusp $\iff$ $J_{10} = I_{12} = I_4 = 0$ and $J_{2i} \neq 0$ for some $i \leq 4$.*

(vi) *$C_{F,H}$ has a point of multiplicity at least 4 $\iff$ $J_{2i} = 0$ for all i.*

Proof. In order to prove (i) it is enough to notice that we have $J_{10} = \Delta(C_{F,H})$, see [64]. So from now on we suppose that there is a point of multiplicity at least 2 and that J_{10} vanishes. Because of the geometric nature of the statement we may assume that l is algebraically closed.

First suppose $\mathrm{char}(l) \neq 2$. We may assume that $H = 0$ and it follows from the general theory of invariants of binary forms of degree d that all invariants vanish, that is $J_{2i} = 0$ for all i, if and only if F is unstable in the sense of [57]. This happens if and only if there is a root of order greater than $d/2$, which is 4 in our case, thus proving (vi). See [57] for the relevant theory; of course this statement can also be proved directly and this is done in [55].

So now we have to look at the case $J_{10} = 0$, but $J_{2i} \neq 0$ for some $i \leq 4$. After a transformation, the sextic F may be written as

$$F(X,Z) = X^2 A(X,Z),$$

where

$$A(X,Z) = (a_0Z^3 + a_1XZ^2 + a_2X^2Z + a_3X^3)Z$$

It follows that we have

$$I_4 = -2^4a_0^2I_4',\ I_{12} = 2^{12}a_0^6a_3^2I_{12}', \tag{3.20}$$

where $I_4', I_{12}' \in l[a_0, a_1, a_2, a_3]$. More precisely, we have $I_4' = 3a_1a_3 - a_2^2$ and if $a_3 \neq 0$, then we get

$$a_3^2I_{12}' = \Delta(A),\ I_4' = c_4(A),$$

where Δ and c_4 are invariants of binary quartics defined in [39].

We next prove (v). If F has a triple root, then we may assume it is at $X = 0$, so a_0 vanishes and hence $I_4 = I_{12} = 0$. If, conversely, we have $I_4 = I_{12} = 0$, then according to (3.20) we either have $a_0 = 0$, in which case F has a triple root at $X = 0$, or we have $a_0 \neq 0$, but $I_4' = 3a_1a_3 - a_2^2 = 0$ and $a_3I_{12}' = 0$. But if $a_3 = 0$ holds, then we must also have $a_2 = 0$, whereby we have a triple root at $Z = 0$, and if a_3 is nonzero, then $\Delta(A) = c_4(A) = 0$, implying that A must have a triple root. This proves (v).

So now we may assume that $I_4 \neq 0$ or $I_{12} \neq 0$ and moreover $a_0 \neq 0$ and at least one of a_2 or a_3 is nonzero.

For the proof of (ii), notice that we have

$$I_{12} \neq 0 \iff a_3 \neq 0 \text{ and } \Delta(A) \neq 0;$$

but the last condition means that there is no double root except for the one at $X = 0$.

We still have to prove (iii) and (iv), so we suppose that $a_3 = 0 = I_{12}$, but $a_0a_2 \neq 0$. The relevant invariants are

$$J_4 = 2^{-7}(4a_0a_2 - a_1^2)(4a_0a_2 - 3a_1^2)$$

and

$$J_6 = 2^{-10}(4a_0a_2 - a_1^2)a_1^2$$

and the result follows, since F has 3 double roots if and only if $4a_0a_2 = a_1^2$.

Now we deal with the case of characteristic 2. We have $J_{10} = 0$ and there is a point $P \in C_{F,H}(l)$ of multiplicity $\delta(P, C_{F,H}) \geq 2$. We move it to $P_0 = (0:0:1)$ and apply a suitable transformation to ensure that all the f_i vanish for even i, so F and H are of the form

$$\begin{aligned} H(X,Z) &= X(h_1Z^2 + h_2XZ + h_3X^2), \\ F(X,Z) &= X^3Z(f_3Z^2 + f_5X^2). \end{aligned}$$

Hence we have $\delta(P_0, H) \geq 1$ and $\delta(P_0, F) \geq 3$ by (3.18) and we shall use that in this case J_2 is equal to $h_1^2h_2^2$.

We first prove (vi). If there is some $P \in C_{F,H}(l)$ such that $\delta(P, C_{F,H}) \geq 4$, we may move it to P_0 and transform F and H so that $\delta(P_0, H) \geq 2$ and $\delta(P_0, F) \geq 4$, which means that $h_1 = f_3 = 0$. One checks easily that this implies $J_{2i} = 0$ for all i.

If, on the other hand, all J_{2i} vanish, then in particular J_2 vanishes, so we either have $h_1 = 0$ or $h_2 = 0 \neq h_1$. Assuming $h_1 = 0$ we deduce $J_4 = J_6 = 0$ and $J_8 = f_3^8$, so we find $f_3 = 0$ and hence P_0 has multiplicity at least 4.

The situation $h_2 = 0 \neq h_1$ is more difficult, since we have $\delta(P_0, C_{F,H}) = 2$ and hence the point of multiplicity 4 we are looking for is not P_0; here we have $J_6 = h_1^6(f_5 h_1 + f_3 h_3)^2$, and thus $f_3 h_3 = f_5 h_1$. Hence we find $J_8 = f_3^4(f_3^2 + h_1^3 h_3)^2$, so either $f_3 = 0$ or $f_3^2 = h_1^3 h_3 \neq 0$. Notice that $H = X(h_1 Z^2 + h_3 X^2) = XH'(X, Z)$, where H' is a square, say $H'(X, Z) = G(X, Z)^2$.

If f_3 vanishes, then f_5 also vanishes and we find $F = 0$. But according to (3.18) this means that the point $(X_0 : 0 : Z_0)$ has multiplicity 4, where $G(X_0, Z_0) = 0$.

Conversely, if $f_3^2 = h_1^3 h_3 \neq 0$ holds, then $h_3 \neq 0$, so there is some $x_0 \in l^*$ satisfying

$$G(x_0, 1) = 0. \tag{3.21}$$

Without loss of generality we may assume $h_3 = 1$ and thus $h_1 = x_0^2$, implying $f_3 = f_5 x_0^2$ and $f_3^2 = x_0^6$. Therefore we deduce $f_3 = x_0^3$ and $f_5 = x_0$, whereby F can be written as

$$F(X, Z) = x_0 X^3 Z(X + x_0 Z)^2.$$

Hence the point $Q = (x_0 : 0 : 1)$ lies in $C_{F,H}(l)$ and satisfies both $\delta(Q, H) = 2$ and $\delta(Q, F) = 2$. So we have $\delta(Q, C_{F,H}) > 2$ (see (3.19)) and in order to compute $\delta(Q, C_{F,H})$ we need to apply a transformation, in the course of which we may move Q to P_0. But this means that the new H satisfies $h_0 = h_1 = 0$ and we can proceed as before to show $f_3 = 0$ and thus $\delta(Q, C_{F,H}) = 4$. This proves (vi).

From now on it suffices to look at $C_{F,H}$ satisfying $\delta(P, C_{F,H}) \leq 3$ for all $P \in C_{F,H}(l)$ and $J_{2i} \neq 0$ for some $i < 5$. We observe that we have

$$I_4 = h_1^4 h_2^4 \text{ and } I_{12} = h_1^8 I'_{12},$$

where I'_{12} lies in $l[h_1, h_2, h_3, f_3, f_5]$.

We follow the same strategy employed in the case $\mathrm{char}(l) \neq 2$, so we proceed by proving part (v). Suppose there is a point of multiplicity 3 which we can assume to be P_0. Then we have $h_1 = 0$ and hence $I_4 = I_{12} = 0$.

Conversely, suppose both I_4 and I_{12} vanish. Then either $h_1 = 0$ holds, which implies $\delta(P_0, C_{F,H}) = 3$, or $h_2 = 0 \neq h_1$ and $I_{12} = h_1^{12}(f_5 h_1 + f_3 h_3)^4 = 0$, and thus

$$f_5 h_1 + f_3 h_3 = 0. \tag{3.22}$$

Moreover, $h_2 = 0$ and (3.22) imply $J_2 = J_4 = J_6 = 0$ and $J_8 = f_3^4(h_1^3 h_3 + f_3^2)$, so in particular f_3 must be nonzero. It follows from (3.22) that either $f_5 = h_3 = 0$ and $\delta(\infty, C_{F,H}) = 0$, where $\infty = (1:0:0)$, or $f_5 \neq 0 \neq h_3$. In the latter situation, let us assume without loss of generality that we have $h_3 = 1$ and let x_0 be defined as in (3.21). Then (3.22) implies $f_3 = f_5 h_1$ and hence we get

$$F(X,Z) = f_5 X^3 Z(X + x_0 Z)^2.$$

As in the proof of (vi) this means that we have $\delta(Q,H) = \delta(Q,F) = 2$, where $Q = (x_0 : 0 : 1) \in C_{F,H}(l)$. Thus we must have $\delta(Q, C_{F,H}) > 2$ because of (3.19), so $\delta(Q, C_{F,H}) = 3$ and part (v) is proved.

For the rest of the proof we deal with $C_{F,H}$ such that $\delta(P, C_{F,H}) \leq 2$ for all $P \in C_{F,H}(l)$ and either $I_4 \neq 0$ or $I_{12} \neq 0$. Because of $\delta(P_0, F) \geq 3$, H is not of the form $h_3 X^3$, so we may move one of the other roots to ∞. As before, we have $h_1 \neq 0$, so we may assume

$$H(X,Z) = XZ(Z + h_2 X).$$

We know $\delta(P_0, C_{F,H}) = 2$ and we want to check whether there are any other points $P \in C_{F,H}(l)$ satisfying $\delta(P, C_{F,H}) = 2$. Using the substitution $Y = XY'$, we see that this is the case if and only if the projective cubic curve defined by the affine equation

$$C'_{F',H'} : Y'^2 + (1 + h_2 X)Y' = X(f_3 + f_5 X^2)$$

has a node. Now an easy computation reveals $I'_{12} = h_2^4 \Delta(C_{F',H'})$, proving part (ii).

For the final part of the proof we assume that $I_{12} = 0 \neq I_4$ and there are at least two points of multiplicity 2. We can move one of them to ∞ and act on $C_{F,H}$ using an element of $GL_2(l)$ to get

$$\begin{aligned} H(X,Z) &= XZ(X+Z), \\ F(X,Z) &= f_3 X^3 Z^3. \end{aligned}$$

It suffices to compute J_4 and J_6 which turn out to satisfy

$$\begin{aligned} J_4 &= f_3(1 + f_3), \\ J_6 &= f_3^2(1 + f_3)^2, \end{aligned}$$

so if $f_3 \neq 0, 1$, we are in case (iii); if $f_3 = 0$, then obviously $\delta(R, C_{F,H}) = 2$ for $R = (1:0:1) \in C_{F,H}(l)$ and if $f_3 = 1$, we move R to P_0 to complete the proof. □

Remark 3.40. The second part of the proof of Theorem 3.39 gives some partial justification for some of our choices of representatives in Section 3.4.4.

Remark 3.41. Igusa invariants are implemented in `Magma`. Because the formulas defining Igusa invariants are quite complicated, it is usually better to use a quicker method called Überschiebung to compute certain related invariants defined by Clebsch in [22]; the Igusa invariants can be expressed as simple polynomials in the Clebsch invariants. This is all described in [70]. However, if the characteristic of the ground field is equal to 2, 3 or 5, then the Clebsch invariants all vanish and we must use explicit formulas for the Igusa invariants themselves.

Remark 3.42. Let k be a number field. We can use Theorem 3.39 to analyze the reduction of a genus 2 curve modulo non-archimedean places v. However, this is not so helpful if we only deal with one place v at a time, because either Igusa invariants have to be computed anew over each relevant k_v which is not very efficient or we can compute them over each relevant residue field $\mathfrak{k}_v$ - but then we cannot use Überschiebungen unless $v(30)$ equals zero. Hence it is usually better to compute the invariants once over k using Überschiebungen and reduce them for several places. This is usually faster than factorization over each residue field.

Remark 3.43. Another application of Igusa invariants is a sufficient criterion for v-minimality: If C is a genus 2 curve given by an equation of the form (3.13) over k_v as above, then C is a v-minimal equation of this form if there is some i such that $v(J_{2i}(C)) < 2i$, see [70]. Yet all models that we consider from now on are v-minimal in the sense of [62], since we can restrict to models that have no point of multiplicity ≥ 4 using Proposition 3.36.

3.6 Formulas for local error functions

In this section we consider a non-archimedean place v. We try to find explicit formulas for $\varepsilon_v(P)$ and $\mu_v(P)$ for the five cases introduced at the end of Section 3.4.4. Our main tool is the explicit description of the respective Néron models that we can compute easily in all cases.

So let C be a smooth projective curve of genus 2 defined over k_v and given as the smooth projective model of an equation of the form 3.13, where F and H are as in one of the 5 cases from Section 3.4.4. These models are v-minimal models in the sense of [63]; this follows easily from Remark 3.43. Moreover, their closures are always normal; this can be verified using Serre's "$R_1 + S_2$"–criterion proved in [65, Chapter 8, Theorem 2.23].

In order to compute the component groups Φ_v, we use Proposition 1.37. For the relevant computations we need to be able to compute the intersection matrix of the special fiber $\mathcal{C}_v$ of a proper regular model of C over $\mathrm{Spec}(\mathcal{O}_v)$; algorithmically this can be done using `Magma`. In fact we determine the minimal proper regular model $\mathcal{C}_v^{\min}$ in all cases; it always satisfies condition (†) (see Remark 1.35).

We prove very little in this section, the complete proofs can be found in Appendix A. Our main reference for the different reduction types we encounter is the article of Namikawa and Ueno [76]. Some of the results of this section yield improvements to Stoll's height constant bound from Proposition 3.11 and we mention these in passing.

In cases (1), (2) and (3) the proofs in the appendix are given only for $v(2) = 0$, since the complementary case is very similar and follows easily from changing a few of the explicit congruences used in the proofs. In these cases the given model is clearly semistable and hence has rational singularities (see Example 1.23), whereby ε_v and μ_v factor through Φ_v because of Theorem 3.30.

However, in the proofs of Theorems 3.62 and 3.74 for cases (4) and (5) there are some more essential differences, so we give at least some parts of the proofs of these theorems for both $\mathrm{char}(\mathfrak{k}_v) = 2$ and $\mathrm{char}(\mathfrak{k}_v) \neq 2$. Here we do not always have rational singularities on the closure of the given model, but we can characterize when this is the case. In general we find formulas for $\mu_v(P)$, where P lies in a subgroup of $J(k_v)$ whose index is always at most 4, except for one special reduction type. The quadraticity of $\hat{\lambda}_v$ (see Proposition 3.23) can then be used to compute $\mu_v(P)$ for any $P \in J(k_v)$.

For the remainder of this section we assume that $x = (x_1, x_2, x_3, x_4)$ is a set of v-integral Kummer coordinates for a point $P \in J(k_v)$ such that one of the x_i has valuation equal to zero and that $\varepsilon_v(P) > 0$. Let π denote a uniformizer of $\mathcal{O}_v$.

3.6.1 Case (1)

We let $m = v(\Delta)$. If $m = 1$, then the reduction of C, a curve A of genus 1 with a node, is regular. In general, there is a unique component, which we denote by A, of genus one in the special fiber of $\mathcal{C}_v^{\min}$. As in the case of multiplicative reduction of elliptic curves (see for example [89]) the singular point on the special fiber is replaced by a string of $m - 1$ components of $\mathcal{C}_v^{\min}$, all of genus zero and multiplicity one.

We define a map $\phi : C(k_v) \to \mathbb{Z}/m\mathbb{Z}$ by setting $\phi(Q) = j$ if Q maps to the jth component B_j of the special fiber $\mathcal{C}_v^{\min}$, where, in the notation introduced above, $A = B_0$ is the 0th component, B_1 and B_{m-1} are the components intersecting A and the other components are numbered consecutively, see Figure 3.1. In the notation of Namikawa and Ueno this is reduction type $[I_{m-0-0}]$ (cf. [76]).

Then, using Proposition 1.37, it is easy to see that the component group Φ_v of the Néron model is generated by $[B_1 - A]$ or by $[B_{m-1} - A]$ and is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. We fix one of these generators, say $[B_1 - A]$.

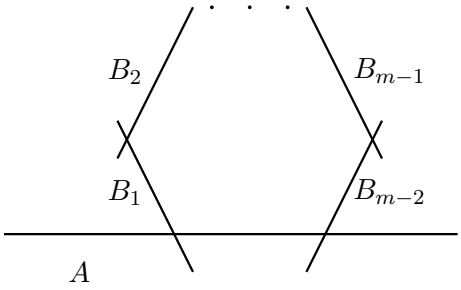

Figure 3.1: The special fiber of reduction type $[I_m - 0 - 0]$

We define the map $\chi : J(k_v) \to \mathbb{Z}/m\mathbb{Z}$ by

$$\chi(P) = i \quad \text{if } P \text{ maps to } [B_i - A].$$

If we have $v(2) = 0$ and $H = 0$, we can apply a suitable transformation of the form $([1, 0, c, 1], 1, 0)$, where $c \in k_v$, so that we are in the situation

$$m = \min\{v(f_6), 2v(f_5)\}. \tag{3.23}$$

Remark 3.44. If (3.23) does not hold, then we have

$$m = v(f_4 f_6 - f_5^2) > \min\{v(f_6), 2v(f_5)\}$$

and so $v(f_6) = 2v(f_5) =: i$, because $v(f_4) = 0$. We can find c as follows: Let $f_6 = f_6' \pi^{2i}$ and $f_5 = f_5' \pi^i$, where $v(f_5') = v(f_6') = 0$. If there is a solution to the congruence $f_4 c'^2 - f_5' c' + f_6' \equiv 0 \pmod{\pi}$, then we lift c' to k_v in such a way that $v(f_4 c^2 - f_5 c + f_6) = 2i + 1$, which is odd. If there is no such solution, then we simply lift $c' = \frac{f_5'}{2f_4}$ to k_v. In both cases we apply the transformation $\tau = ([1, 0, c, 1], 1, 0)$ and it is easy to see that this ensures that the model of C given by $Y^2 = \tau^* F(X, 1)$ satisfies our assumption.

Remark 3.45. In case of residue characteristic 2 we have to work a bit harder. Our goal is, however, the same; we want to make sure that we have $m = \min\{v(f_6), 2v(f_5)\}$. Looking at the formula for the discriminant, we see that if $2v(h_3)$ is larger than m, then $m = v(f_6 h_2^2 - f_5^2)$, so we have to make sure that

$$v(f_6 h_2^2 - f_5^2) = \min\{v(f_6), 2v(f_5)\}$$

holds.

It is not hard to see that both can be achieved simultaneously using a transformation $([1, 0, c, 1], 1, u_3 X^3)$, where c and u_3 are chosen so that they satisfy

$$\begin{aligned} H(X, cZ) + 2u_3 X^3 &\equiv 0 \pmod{\pi^{\lfloor m/2 \rfloor + 1}} \\ \frac{\partial F}{\partial Z}(X, cZ) + u_3 \frac{\partial H}{\partial Z}(X, cZ) &\equiv 0 \pmod{\pi^{\lceil m/2 \rceil}}. \end{aligned}$$

These congruences are not difficult to solve in practice, since we may take an unramified extension, if necessary.

Having ensured that we have $m = \min\{v(f_6), 2v(f_5)\}$, we define

$$w(P) := \min\{v(x_1), v(x_4), m/2\}. \tag{3.24}$$

Notice that $Q \in C(k_v)$ maps to $A = B_0$ if and only if $v(z(Q)) \leq 0$, where $z(Q) = Z(Q)/X(Q)$. Furthermore, tracing the blow-ups required to build the special fiber $\mathcal{C}_v^{\min}$, we see that if $0 < v(z(Q)) < m/2$, then a point $Q \in C(k_v)$ maps to one of the components B_i or B_{m-i} if and only if $v(z(Q)) = i$ and that if m is even, Q maps to $B_{m/2}$ if and only if $v(z(Q)) \geq m/2$. If m is odd, then necessarily $v(z(Q)) < m/2$.

Because the model is semistable, we can extend the field and then the only difference is that m is multiplied by the ramification index of the extension. Hence we may assume that any given $P \in J(k_v)$ is of the form $P = [(P_1) - (P_2)]$ with $P_i \in C(k_v)$. The proofs of the next two lemmas are provided in Appendices A.4 and A.5.

Lemma 3.46. *We have*

$$\varepsilon_v(P) = 2\min\{\chi(P), m - \chi(P)\}.$$

Now we want to relate $w(P)$ to $\chi(P)$ and $\varepsilon_v(P)$.

Lemma 3.47. *We have*

$$\varepsilon_v(P) = 2w(P),$$

and in particular

$$w(P) = \min\{\chi(P), m - \chi(P)\}.$$

The next lemma enables us to deduce a formula for $\mu_v(P)$.

Lemma 3.48. *Let G be an abelian group and let $\varepsilon : G \longrightarrow \mathbb{R}$ be a function. Then there exists at most one bounded function $\mu : G \longrightarrow \mathbb{R}$ satisfying*

$$4\mu(g) - \mu(2g) = \varepsilon(g). \tag{3.25}$$

for all $g \in G$.

Proof. Suppose that we have two bounded functions μ and μ' satisfying (3.25) and that there is some $g_0 \in G$ such that $\mu(g_0) \neq \mu'(g_0)$, say

$$\mu(g_0) - \mu'(g_0) = d_0 \neq 0.$$

The function $\nu := \mu - \mu'$ satisfies

$$4\nu(g) - \nu(2g) = 0$$

for all $g \in G$. Hence we have

$$\nu(2^n g_0) = 4^n \nu(g_0) = 4^n d_0$$

for any $n \geq 0$, contradicting the assumption that μ and μ' are bounded. □

Proposition 3.49. *We have*

$$\mu_v(P) = \frac{w(P)(m - w(P))}{m}.$$

Proof. Let $\mu'_v(P) = \frac{w(P)(m-w(P))}{m}$. Then we find

$$4\mu'_v(P) - \mu'_v(2P) = 2w(P) = \varepsilon_v(P)$$

for all $P \in J(k_v)$. But we also have, by definition of μ_v,

$$4\mu_v(P) - \mu_v(2P) = \varepsilon_v(P)$$

for all $P \in J(k_v)$. Since both μ_v and μ'_v are bounded, we can use Lemma 3.48 to finish the proof. □

The discussion of this section shows that we get the following bounds on the height constant β_v.

Corollary 3.50. *Suppose that C/k_v is a smooth projective genus 2 curve such that there is a unique node in the reduction of C. Then we have*

$$m \text{ even} \quad \Rightarrow \quad \beta_v \leq \frac{m}{4},$$

$$m \text{ odd} \quad \Rightarrow \quad \beta_v \leq \frac{m^2 - 1}{4m}.$$

Proof. The bounds are clear for curves of the form considered in Proposition 3.49. For other curves one has to analyze the behavior of μ_v under transformations, see Corollary 3.25. We find

$$\beta_v(C) \leq \beta_v(\tau(C)) + \rho_v(\tau) - v(\tau),$$

where

$$\rho_v(\tau) = \sup\{v(\tau(x)) : x \in K_{\mathbb{A}}, v(x) = 0\}.$$

However, all transformations required to transform a model whose reduction has a unique node into a model for which Proposition 3.49 is applicable satisfy $v(\tau) = \rho_v(\tau) = 0$. □

Remark 3.51. If the residue characteristic is not 2, then the bounds from Corollary 3.50 are better than the bound $\beta_v \leq \frac{m}{3}$ predicted by Proposition 3.11. If $v(2) > 0$, then it is not so easy to compare the bounds, because Proposition 3.11 requires a model of the form $H = 0$. However, if we have a model that violates this, then we can compare our result to the bound predicted by Proposition 3.11 for the model

$$\tau(C) : Y^2 = 4F(X, 1) + H(X, 1)^2,$$

see Section 3.3. Then we have $v(\tau^{-1}) = -2v(2)$ and $\rho_v(\tau^{-1}) = 0$, implying

$$\beta_v(\tau(C)) \leq \beta_v(C) + 2v(2).$$

So if m is even, say, then we get $\frac{m}{4} + 2v(2)$, which is certainly smaller than the bound $\frac{m+16v(2)}{3}$ that we obtain from 3.50.

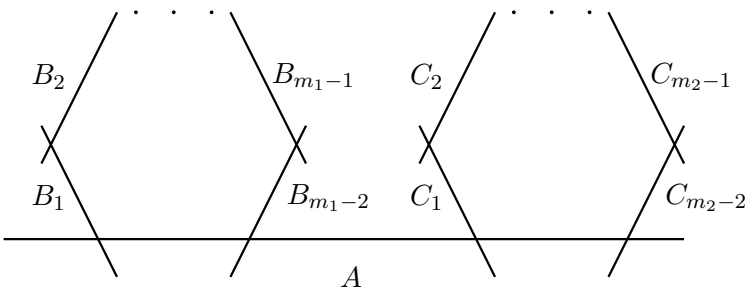

Figure 3.2: The special fiber of reduction type $[I_{m_1-m_2-0}]$

3.6.2 Case (2)

In this case there are two nodes in the reduction. If the residue characteristic is not 2, then, using Hensel's Lemma, we can factor F into a product of quadratic forms

$$F(X,Z) = F_1(X,Z)G(X,Z)F_2(X,Z),$$

where

$$F_1 \equiv Z^2,\ G \equiv (X-Z)(X-aZ),\ F_2 \equiv X^2 \pmod{\pi}$$

such that

$$v(\mathrm{disc}(F_1)) = m_1,\ v(\mathrm{disc}(G)) = 0,\ v(\mathrm{disc}(F_2)) = m_2$$

and the resultants between the quadratic forms have valuation equal to zero. Hence we have $v(\Delta) = m_1 + m_2$.

If $\mathrm{char}(\mathfrak{k}_v) = 2$, then we also have $v(\Delta) = m_1 + m_2$, where m_1 and m_2 correspond to the respective singular points. In order to compute the m_i, we can use a transformation to ensure $v(h_0) \gg 0$ and $v(h_3) \gg 0$; then we get $m_1 = v(f_6h_2^2 - f_5^2)$ and $m_2 = v(f_0h_1^2 - f_1^2)$. Of course, if we know the valuation of the discriminant already, we only need to compute one of the m_i.

In this situation we find that the special fiber of $\mathcal{C}^{\min}$ is obtained by blowing up the two singular points of the special fiber of the closure of C repeatedly and replacing them with a chain of $m_1 - 1$ and $m_2 - 1$ curves of genus 0, respectively; see the discussion of case (1). We call these components $B_1, \ldots, B_{m_1-1}, C_1, \ldots, C_{m_2-1}$, numbered as in Figure 3.2, where A contains all images of points reducing to a regular point modulo π. The component group Φ_v of the Néron model of J over $\mathrm{Spec}(\mathcal{O}_v)$ can be shown to be isomorphic to $\mathbb{Z}/m_1Z \times \mathbb{Z}/m_2\mathbb{Z}$ and generated by $[B_1 - A]$ and $[C_1 - A]$ using Proposition 1.37. The reduction type is $[I_{m_1-m_2-0}]$ in the notation of

[76]. If we have $m_1 = 1$ or $m_2 = 1$, then the corresponding singular point on the closure of C is regular and therefore is not blown up.

We consider the map

$$\chi(P) = (\chi_1(P), \chi_2(P)) : J(k_v) \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \cong \Phi_v$$

defined by

$$\begin{aligned}
\chi(P) &= (i,j) \quad \text{if } P \text{ maps to } [B_i - C_{m_2-j}],\\
\chi(P) &= (i,0) \quad \text{if } P \text{ maps to } [B_i - A],\\
\chi(P) &= (0,j) \quad \text{if } P \text{ maps to } [C_j - A],\\
\chi(P) &= (0,0) \quad \text{if } P \text{ maps to } 0.
\end{aligned}$$

Remark 3.52. For the computation of μ_v and ε_v, we want to assume, similarly to case 1, that we are in the situation $m_1 = \min\{v(f_6), 2v(f_5)\}$ and $m_2 = \min\{v(f_0), 2v(f_1)\}$. If $v(2) = 0$, we can always use a transformation of the form $([1, b, c, 1], 1, 0)$ in order to reduce to this situation. We can find b and c as in Remark 3.44.

If the residue characteristic is 2, we can use a transformation of the form $\tau = ([1, b, c, 1], 1, u_0Z^3 + u_3X^3)$, see Remark 3.45. We can also use the same method employed there, because we can compute m_1 and m_2 a priori.

As we only care about points for which ε_v does not vanish, we suppose that $v(x_4) > 0$ and in addition $v(x_1) > 0$ or $v(x_3) > 0$. We can now define, similarly to (3.24):

$$w_1(P) := \min\{v(x_1), v(x_4), m_1/2\}, \quad w_2(P) := \min\{v(x_3), v(x_4), m_2/2\}.$$

Lemma 3.53. *Under the given conditions we have*

$$\begin{aligned}
\varepsilon_v(x) &= 2(\min\{\chi_1(P), m_1 - \chi_1(P)\} + \min\{\chi_2(P), m_2 - \chi_2(P)\})\\
&= w_1(P) + w_2(P).
\end{aligned}$$

See Appendix A.6 for the proof. Using Lemma 3.53, we can compute $\mu_v(P)$.

Proposition 3.54. *We have*

$$\mu_v(P) = \frac{w_1(P)(m_1 - w_1(P))}{m_1} + \frac{w_2(P)(m_2 - w_2(P))}{m_2}.$$

Proof. The proof is the same as the proof of Proposition (3.49) if we consider the summands separately. □

The height constant β_v can be bounded as follows:

Corollary 3.55. *Suppose that C/k_v is a smooth projective genus 2 curve such that there are exactly two nodes in the reduction of C. Then we have*

$$\begin{aligned} m_1, m_2 \text{ even} &\Rightarrow \beta_v \leq \frac{m_1+m_2}{4}, \\ m_1 \text{ even}, m_2 \text{ odd} &\Rightarrow \beta_v \leq \frac{m_1}{4} + \frac{m_2^2-1}{4m_2}, \\ m_1, m_2 \text{ odd} &\Rightarrow \beta_v \leq \frac{m_1^2-1}{4m_1} + \frac{m_2^2-1}{4m_2}. \end{aligned}$$

Proof. See the proof of Corollary 3.50. □

Corollary 3.55 gives a nontrivial improvement of the bound

$$\beta_v \leq \frac{m_1+m_2}{3}$$

for the height constant predicted by Proposition 3.11 when $v(2) = 0$. We also get an improvement for the case of residue characteristic 2 as in Remark 3.51.

3.6.3 Case (3)

Although we also have semistable reduction in this case, it is quite different from the two cases discussed above, because the reduction of the curve modulo π has two components to start with. We call these components A and E, and we assume that an affine point (ξ, η) on A satisfies $\eta = \xi(\xi - 1)$.

If $v(2) = 0$, then we can use Hensel's Lemma to factor $F(X, Z)$ as

$$F(X, Z) = F_1(X, Z)F_2(X, Z)F_3(X, Z)$$

such that

$$F_1 \equiv Z^2,\ F_2 \equiv (X - Z)^2,\ F_3 \equiv X^2 \pmod{\pi}$$

and the resultants between distinct F_i have valuation equal to zero. Let m_i denote the valuation of the discriminant of F_i, so $v(\Delta)$ decomposes as $v(\Delta) = m_1 + m_2 + m_3$.

If we are in the situation $v(2) > 0$, then also $v(\Delta) = m_1+m_2+m_3$, where m_1 and m_3 correspond to the singular points at infinity and at $(0 : 0 : 1)$, respectively. A method for the computation of m_1 and m_3 is described in the discussion of case (2) and we compute m_2 either as $m_2 = v(\Delta)-m_1-m_3$ if we know $v(\Delta)$ or using a transformation that moves the singular point at $(1 : 0 : 1)$ to ∞, say.

The special fiber of the minimal proper regular model is obtained using a sequence of blow-ups of the singular points; they are replaced by a chain of $m_i - 1$ curves of genus 0 and simple multiplicity, respectively. Hence

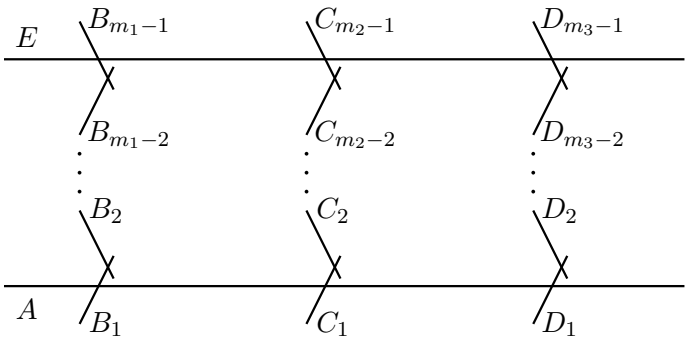

Figure 3.3: The special fiber of reduction type $[I_{m_1-m_2-m_3}]$

the special fiber $\mathcal{C}_v^{\min}$ contains the two components A and E, connected by three chains of curves of genus 0 that we call $B_1, \ldots, B_{m_1-1}$, $C_1, \ldots, C_{m_2-1}$ and $D_1, \ldots, D_{m_3-1}$, respectively, where B_1, C_1 and D_1 intersect A and all intersections are transversal, as shown in Figure 3.3.
Looking for the group Φ_v of connected components of the Néron model of J, we first assume that $m_i > 1$ holds for all i. Then Proposition 1.37 says that Φ_v is isomorphic to the degree zero part of the following group

$$\begin{aligned} L := \langle A, B_1, \ldots, B_{m_1-1}, C_1, \ldots, C_{m_2-1}, D_1, \ldots, D_{m_3-1}, E : \\ 3A = B_1 + C_1 + D_1 \ , \ 3E = B_{m_1-1} + C_{m_2-1} + D_{m_3-1}, \\ 2B_1 = A + B_2 \ , \ 2B_2 = B_1 + B_3, \ \ldots, \ 2B_{m_1-1} = B_{m_1-2} + E, \\ 2C_1 = A + C_2 \ , \ 2C_2 = C_1 + C_3, \ \ldots, \ 2C_{m_2-1} = C_{m_2-2} + E, \\ 2D_1 = A + D_2 \ , \ 2D_2 = D_1 + D_3, \ \ldots, \ 2D_{m_3-1} = D_{m_3-2} + E \ \rangle. \end{aligned}$$

As before, a singular point on the original special fiber corresponding to $m_i = 1$ for some i is regular and therefore not blown up. So if $m_i = 1$ for some i, say $m_1 = 1$, then there is no B_i and instead A and E intersect at the regular point ∞. Hence there are no relations in the third line, and the relations in the second line become $3A = E + C_1 + D_1$ and $3E = A + C_{m_2-1} + D_{m_3-1}$. This, however, does not affect what we do in the following.

Projecting away from A we find, using elementary group theory:

$$\Phi_v \cong \langle B_1, C_1 : m_1 B_1 = m_2 C_1 \ , \ (m_1 + m_3) B_1 = -m_3 C_1 \rangle$$

Now let d denote the greatest common divisor of m_1, m_2 and m_3 and set $n = (m_1 m_2 + m_1 m_3 + m_2 m_3)/d$. Then we can conclude from the above-mentioned isomorphism that

$$\Phi_v \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

As in case (2) we would like to assume $m_1 = \min\{v(f_6), 2v(f_5)\}$ and $m_3 = \min\{v(f_0), 2v(f_1)\}$. We use the same transformation as in case (2) (see Remark 3.52) to ensure that we can always reduce to this situation.

One peculiarity of the present reduction type lies in the nontriviality of ε_v on points on the Jacobian that map to regular points not lying on the connected component of the identity. These are precisely the points $P = [(P_1) - (P_2)]$ such that P_1 and P_2 map to distinct components of the reduction of C. This phenomenon has already been discussed in the proof of Proposition 3.12.

Proposition 3.56. *Suppose $P = [(P_1) - (P_2)] \in J(k_v)$ such that $\varepsilon_v(P) > 0$, let $0 < i < m_3/2$ and $0 < j < m_1$ and let $\xi(P_l)$ denote the component of the special fiber of $\mathcal{C}^{\min}$ that P_l maps to. Moreover, let*

$$v_0 = v(f_3^2 + f_3h_1h_2 - 4f_2f_4 - f_2h_2^2 - f_4h_1^2),$$

let m_4 be defined by

$$\min\{i + v_0, i + v(f_1), i + v(f_0), v(f_5), v(f_6) - i, m_1 - i\}$$

and let m_5 be defined by

$$\min\{2i + 2j + v_0, 2i + v(f_0), 2j + v(f_6), 2i + 2j + v(f_1), 2i + 2j + v(f_5)\}.$$

Then, possibly after applying a suitable transformation, Table 3.3 gives formulas for $\varepsilon_v(P)$ in all cases.

Proof. See Appendix A.7. □

Remark 3.57. Tracing through the proof of Proposition 3.56 given in Appendix A.7 we can determine which component our point P maps to quite easily. We first assume that neither P_1 nor P_2 map to a component C_i. Let $v_1 := \min\{v(x_1), m_1/2\}$ and $v_3 := \min\{v(x_3), m_3/2\}$.

- If $v_1 = v_3 = 0$, then P maps to $\pm[A - E]$.
- If $v_1 = 0, v_3 = i > 0$ and $v(x_4) = v_3$, then P maps to $\pm[D_i - A]$.
- If $v_1 = 0, v_3 = i > 0$ and $v(x_4) > v_3$, then P maps to $\pm[D_i - E]$.
- If $v_1 = j > 0, v_3 = 0$ and $v(x_4) = v_1$, then P maps to $\pm[B_j - A]$.
- If $v_1 = j > 0, v_3 = 0$ and $v(x_4) > v_1$, then P maps to $\pm[B_j - E]$.
- If $v_1 = j > 0, v_3 = i > 0$ and $v(x_4) = v_1 + v_3$, then P maps to $\pm[B_i - D_j]$.
- If $v_1 = j > 0, v_3 = i > 0$ and $v(x_4) > v_1 + v_3$, then P maps to $\pm[B_i - D_{m_1-j}]$.

If one of the P_l maps to some C_i, then we can use the same case distinction after applying an appropriate transformation.

$\xi(P_1)$	$\xi(P_2)$	$\varepsilon_v(P)$
A	E	$\min\{m_1, m_2, m_3\}$
D_i	A	$2i$
D_i	E	$i + m_4$
D_i	$B_j, j \leq m_1/2$	$i + j$
D_i	$B_j, j > m_1/2$	m_5

Table 3.3: Formulas for ε_v in case (3)

Unfortunately we have not been able to find a simple formula for μ_v from our formulas for ε_v as in cases (1) or (2), although such a formula presumably exists. In practice we first compute all possible values of $\varepsilon_v(P)$. Using our explicit description of the component group Φ_v given in the beginning of this section, we can then compute the value of μ_v on any component once and for all as a finite sum plus a finite sum of geometric series, see [94, §6]. Given a point $P \in J(k_v)$ it therefore suffices to determine which component our point lies on to find $\mu_v(P)$.

Remark 3.58. Because we do not have formulas for $\mu_v(P)$, we cannot say anything about the height constant in general. Given a specific curve whose reduction contains 3 nodes we can, however, compute all $\mu_v(P)$ that can possibly occur using the results of this section.

3.6.4 Case (4)

Up to this point Theorem 3.30 has applied to all models we have had to consider. This is about to change and indeed we shall see that new complications arise at once.

Let E denote the elliptic curve given by the Weierstrass equation

$$Y^2Z + h_0f_3Y + h_1XY = X^3 + f_2X^2 + f_1f_3X + f_0f_3^2 \tag{3.26}$$

and let E' denote the elliptic curve given by the Weierstrass equation

$$Y^2Z + h_3f_3Y + h_2XY = X^3 + f_4X^2 + f_5f_3X + f_6f_3^2. \tag{3.27}$$

According to Tate's algorithm reproduced in [89, §IV.9] the reduction type of E' is I_0, since the reduction of the given equation is nonsingular, so in particular the valuation of its discriminant vanishes. Let $\mathcal{K}$ denote the Kodaira symbol for the reduction type of E.

The curve C has reduction type $[I_0 - \mathcal{K} - l]$ for some $l \geq 0$ and $\Delta(C)$ equals the discriminant of the given model of E.

If we have $l = 0$, then the special fiber $\mathcal{C}_v^{\min}$ is the same as the special fiber of reduction type $\mathcal{K}$, but one of the rational curves of multiplicity 1

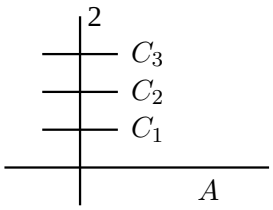

Figure 3.4: The special fiber of reduction type $[I_0 - I_0^* - 0]$

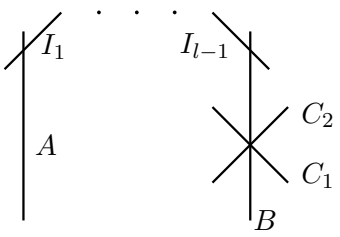

Figure 3.5: The special fiber of reduction type $[I_0 - IV - l]$

is replaced by a curve A of genus 1. We denote the other components of multiplicity 1 in the special fiber of type $\mathcal{K}$, if any exist, by $C_1, \ldots, C_t$, where $t+1 \in \{1, \ldots, 4\}$ is the number of components of K that have simple multiplicity. The case $\mathcal{K} = I_0^*$ is shown in Figure 3.4.

If $l > 0$, then $\mathcal{C}_v^{\min}$ consists of the components making up the special fiber of type $\mathcal{K}$, connected with a genus 1 component A of multiplicity 1 by a chain of $l-1$ curves $I_1, \ldots, I_{l-1}$ of genus 0. Here I_1 intersects A and I_{l-1} intersects a component B of $\mathcal{K}$ of simple multiplicity and the other components of simple multiplicity are denoted $C_1, \ldots, C_t$ as above. See Figure 3.5 for the case $\mathcal{K} = IV$.

Lemma 3.59. *The curve C has a model of the form* (3.13) *whose closure $\mathcal{C}$ has rational singularities if and only if $l = 0$. If $l = 0$, then this holds for the given model of C.*

Proof. We have that the given model of E is v-minimal if and only if $l = 0$. If $\mathcal{C}' \longrightarrow \mathcal{C}$ is a desingularization of $\mathcal{C}$, then it corresponds to a desingularization of the closure of the given model of E, where the strict transform of the nonsingular part is replaced by a curve of genus 1. Now we use Lemma 1.26 which tells us that having rational singularities only depends on the preimage of the singular locus. From Lemma 2.13 we get the second part of the lemma, since the given model is v-minimal if $l = 0$.

If, on the other hand, $l > 0$, then the given equation of E is not v-minimal. In order to make it v-minimal, we need to apply the transformation

τ to the given model of C that acts on affine points (ξ, η) by

$$\tau((\xi, \eta)) = (\pi^{-2l}\xi, \pi^{-3l}\eta).$$

However, applying this transformation to the given equation of E' results in a model of E' that is not v-minimal and so we can again use Lemma 2.13. □

If we have $l = 0$, then Theorem 3.30 and Lemma 3.59 imply that ε_v and μ_v factor through the component group Φ_v of the Néron model. Moreover, it is easy to see that E cannot have multiplicative reduction, so the order of Φ_v is at most 4 and therefore the computation of μ_v becomes particularly easy.

There are several possible ways to do this computation. The most straightforward one consists in computing $\varepsilon_v(P), \varepsilon_v(2P), \varepsilon_v(3P), \varepsilon_v(4P)$ until one of them equals zero and then using the definition of μ_v. However, the following approach, resembling the procedure used for elliptic curves first introduced in [87] (see Theorem 2.17) is faster. We use the multiplication polynomials given by Uchida in [103] for models satisfying $H = 0$ and generalized easily; more precisely the triplication function which we call

$$\psi_3(x) = (\psi_{3,1}(x), \ldots, \psi_{3,4}(x)), \tag{3.28}$$

satisfying:

- If x is a set of Kummer coordinates for $P \in J(k_v)$, then $\psi_3(x)$ is a set of Kummer coordinates for $3P$.
- $\psi_3((0,0,0,1)) = (0,0,0,1)$.
- $\psi_3(x)$ has coefficients in $\mathbb{Z}[f_0, \ldots, f_6, h_0, \ldots, h_3]$.

Note that our $\psi_{3,i}$ is $\mu_{3,i}$ in Uchida's notation. For $x \in K_{\mathbb{A}}(k_v)$ we set

$$\omega_v(x) := v(\psi_3(x)) - 9v(x)$$

and notice that, similarly to ε_v, this function is well defined on $K(k_v)$ and moreover, if we compose it with the usual surjection from J onto K, on $J(k_v)$.

Furthermore, Proposition 3.24 implies

$$\mu_v(3P) = 9\mu_v(P) - \omega_v(P). \tag{3.29}$$

Let us assume that we are given a point $P \in J(k_v)$ and we know that the reduction type of C over $\mathcal{O}_v$ is of the form $[I_0 - \mathcal{K} - 0]$, where $\mathcal{K}$ is some Kodaira type. We also assume $\varepsilon_v(P) \neq 0$.

If $2P \in J_0(k_v)$, then

$$\mu_v(P) = \frac{1}{4}\varepsilon_v(P),$$

but on the other hand we have $\mu_v(3P) = \mu_v(P)$. Therefore (3.29) implies

$$\mu_v(P) = \frac{1}{8}\omega_v(P)$$

and

$$\omega_v(P) = 2\varepsilon_v(P).$$

If $3P \in J_0(k_v)$, then we find

$$\mu_v(P) = \frac{1}{3}\varepsilon_v(P) = \frac{1}{9}\omega_v(P)$$

so that the relation

$$\omega_v(P) = 3\varepsilon_v(P) \tag{3.30}$$

holds.

The final case is $2P, 3P \notin J_0(k_v)$. We have $4P \in J_0(k_v)$ and hence

$$\mu_v(P) = \frac{1}{8}\omega_v(P) = \frac{1}{4}\varepsilon_v(P) + \frac{1}{16}\varepsilon_v(2P).$$

We cannot compute $\mu_v(P)$ directly if we find that (3.30) holds. But if we take a closer look which reduction types are possible in this case, we see that we must have $\mathcal{K} \in \{IV, IV^*\}$ if $3P \in J_0(k_v)$, whereas the complementary case can only occur if $\mathcal{K} = I_n^*$ and n is odd. This means that, at least if $v(6) = 0$, we can tell which case we are in by checking the valuation of the discriminant: For IV, IV^* it is even, whereas for $\mathcal{K} = I_n^*$ it is odd if and only if n is. If the residue characteristic is equal to 2, then we know at least that if $v(\Delta)$ is odd, then we have type I_n^* and hence $3P \notin J_0(k_v)$. Similarly, if the residue characteristic is 3, then we must have reduction type IV or IV^* and hence $3P \in J_0(k_v)$ if $v(\Delta)$ is even. If none of these conditions are satisfied, we simply check $\varepsilon_v(2P)$ and $\varepsilon_v(P)$ for equality.

This leads to Algorithm 2, where $P \in J(k_v)$ and we assume that the reduction of J over $\mathcal{O}_v$ is of the form $[I_0 - \mathcal{K} - 0]$.

Remark 3.60. What about the height constant β_v? If $\#\Phi_v < 4$, then we can use Corollary 3.32 because of Lemma 3.59. If we are in case $\mathcal{K} = IV$ or $\mathcal{K} = IV^*$, then we have $\#\Phi_v = 3$ and if a search for $P \in J(k_v)$ of small height produces no nontrivial $\varepsilon_v(P)$, then we may have $c_v = \#\Phi_v(\mathfrak{k}_v) = 1$ and thus $\beta_v = 0$. See the discussion following Corollary 3.32.

If we have $\#\Phi_v = 4$, then we can proceed as follows: If we find $c_v < 4$, then we are in the situation discussed already. If this does not hold, then we can compute $\varepsilon_v(P)$ for P of small naive height. However, we can only be certain that we have determined all possible values if we find three different values if $\Phi_v \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (in fact, if $\varepsilon_v(P) \neq 0 \neq \varepsilon_v(Q)$, then $\varepsilon_v(P+Q)$ will yield the third value), respectively two if $\Phi_v \cong \mathbb{Z}/4\mathbb{Z}$, taken on by ε_v – unless we can also show somehow that we have found at least one point

Algorithm 2 Computation of $\mu_v(P)$ for reduction type $[I_0 - \mathcal{K} - 0]$

if $\omega_v(P) = 2\varepsilon_v(P)$ **then**
  return $\frac{1}{8}\omega_v(P)$
else if $\omega_v(P) \neq 3\varepsilon_v(P)$ **then**
  return $\frac{1}{8}\omega_v(P)$
else if $v(6) = 0$ **then**
  return $\frac{1}{9-(v(\Delta) \pmod 2)}\omega_v(P)$
else if $v(2) > 0$ and $2 \nmid v(\Delta)$ **then**
  return $\frac{1}{9}\omega_v(P)$
else if $v(3) > 0$ and $2 \mid v(\Delta)$ **then**
  return $\frac{1}{8}\omega_v(P)$
else if $\varepsilon_v(2P) = \varepsilon_v(P)$ **then**
  return $\frac{1}{9}\omega_v(P)$
else
  return $\frac{1}{8}\omega_v(P)$
end if

for each component. But we can get a small improvement even without computing c_v or any ε_v just from knowing the exponent of Φ_v. In case $\Phi_v \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ we have $\mu_v(P) = \frac{1}{4}\varepsilon_v(P)$, so that any bound B for the maximum value γ_v of $|\varepsilon_v|$ yields a bound $\beta_v \leq \frac{B}{4}$ (as opposed to $\frac{B}{3}$). In particular we could use the bound $v(2^4 \operatorname{disc}(F))$ from Proposition 3.11 or one of its improvements discussed in [92, §7]. If we have $\Phi_v \cong \mathbb{Z}/4\mathbb{Z}$, then a similar argument shows that $\beta_v \leq \frac{5}{16}B$, where B is any upper bound for γ_v.

If l is positive and E has additive reduction, the order of the component group is still at most 4. However, according to Lemma 3.59 the closure of the given model of C does not have rational singularities and there is no way to repair this. But because the implication of Theorem 3.30 has not been shown to be an equivalence, this does not necessarily mean that ε_v and μ_v cannot factor through Φ_v and there is some hope left. Yet consider the following example.

Example 3.61. Let p be an odd prime and let C be the smooth projective model of $y^2 = (x^2+1)(x^3 + p^5x + p^8)$ over $\mathbb{Q}_p$. Let $P_1 = (0, p^4) \in C$ and $P_2 = -P_1$. We have reduction type $[I_0 - III - 1]$ and hence $\#\Phi_v = 2$. It turns out that both P_1 and P_2 map to the component C_1 (see the beginning of this section) and so we have $P \in J_0(k_v)$. The image on the Kummer surface is of the form $(x_1, 0, 0, x_4)$, where $v(x_4) - v(x_1) = 2 = 2l$. We get $\varepsilon_v(P) = \varepsilon_v(2P) = 6$ and, in accordance with Theorem 3.62 below, $\mu_v(P) = \mu_v(2P) = 2 = 2l$.

Hence the computation of $\mu_v(P)$ becomes more involved. Still, below we prove a simple formula for $\mu_v(P)$ when $P \in J_0(k_v)$ under some additional conditions which can always be ensured to hold after a simple transforma-

tion.

Theorem 3.62. *Suppose C has reduction type $[I_0 - \mathcal{K} - l]$, where $\mathcal{K}$ is not a multiplicative Kodaira type and $l \geq 0$. Furthermore, suppose that $v(h_0) \geq 3l, v(h_1) \geq l, v(f_0) \geq 6l, v(f_1) \geq 4l, v(f_2) \geq 2l$ and that the only transformation required when applying Tate's algorithm to E is $(\xi, \eta) \mapsto (\pi^{-2l}\xi, \pi^{-3l}\eta)$. Let $x = (x_1, x_2, x_3, x_4)$ be a set of v-integral Kummer coordinates for $P \in J_0(k_v)$ with $v(x_3) > 0$, $v(x_4) > 0$ and either $v(x_1) = 0$ or $v(x_2) = 0$. Then we have*

$$\mu_v(P) = \min\{v(x_3), v(x_4), 2l\}.$$

Proof. See Appendix A.8. □

Remark 3.63. The condition on Tate's algorithm basically amounts to requiring the coefficients h_0, h_1, f_0, f_1, f_2 to have valuation as large as possible simultaneously. In order to satisfy it, we simply apply Tate's algorithm to the given model of E, record the transformations needed and apply them to C. Having done so, we can apply Theorem 3.62 to the resulting Jacobian.

Remark 3.64. We can safely leave out the case $\mathcal{K} = I_n$, $n \geq 1$, because if we have such a curve, then we can apply a transformation producing a model that falls into case (5) and this will be dealt with in Section 3.6.5. This reduction type is easily distinguishable, for example by applying Tate's algorithm to the model of E.

Remark 3.65. The preceding theorem enables us to compute $\mu_v(P)$ for arbitrary P using the fact that we can always find some $n \in \{1, \ldots, 4\}$ such that $nP \in J_0(k_v)$. The number n can be determined quite easily once we have applied the transformations necessary to use the theorem. Finally we note that the case $n = 4$ is generally not very common, so mostly an application of δ or ψ_3 (see (3.28)) suffices. This is in contrast with the fact that we may have to go up to quite large multiples of our point if we want to ensure that ε_v vanishes for this multiple, see the conjecture below.

The proof of Theorem 3.62 given in Appendix A.8 is very elementary but also lengthy. The simplicity of the formulas hints at the existence of a more clever or at least more enlightening proof, possibly using Néron's interpretation of canonical local height pairings and Lang's interpretation of Néron functions as intersection multiplicities that we have already used in the proof of Theorem 3.30.

Recall that if $H = 0$ and $\mathrm{char}(k_v) \neq 2$, then $J^0(k_v)$ consists of the elements of $J(k_v)$ that are nonsingular (when viewed as elements of the given model of J that is defined by 72 quadrics in $\mathbb{P}^{15}$ and that is determined by F) and map to the connected component of the identity of the special fiber of the given model. The group $J^0(k_v)$ depends on the given model and

by Proposition 3.12 equals the group U_v of points on which ε_v vanishes, at least for residue characteristic not equal to 2. Therefore we see that in the present case $J_0(k_v)$ strictly contains $J^0(k_v)$. This phenomenon has also been discussed in a different context by Bruin and Stoll in [13, Remark 5.16]. On a side note, it should be possible to prove Proposition 3.12 in the situation where $\mathrm{char}(\mathfrak{k}_v) = 2$ using the explicit embedding of the Jacobian in $\mathbb{P}^{15}$ for fields of characteristic 2 (and $h_3 = 0$) from [33], but we have not attempted this.

It is natural to ask about the index of $J^0(k_v)$ in $J_0(k_v)$. Experimental data suggests the following:

Conjecture 3.66. *Suppose that k is a global field and that the given model of C is v-minimal with reduction type $[I_0 - \mathcal{K} - l]$, where $\mathcal{K}$ is an additive Kodaira type. Furthermore, suppose that $v(h_0) \geq 3l, v(h_1) \geq l, v(f_0) \geq 6l, v(f_1) \geq 4l, v(f_2) \geq 2l$ and that applying Tate's algorithm to the given equation of E yields no transformations except for $(\xi, \eta) \mapsto (\pi^{-2l}\xi, \pi^{-3l}\eta)$. Then we have $\varepsilon_v(p^l P) = 0$ for all $P \in J_0(k_v)$.*

Note that having reduction type $[I_0 - \mathcal{K} - l]$ means that there is a chain of l projective lines connecting the genus 1 curve coming from E' and the Kodaira type. Each of these $\mathbb{P}^1$s contributes p new points to the special fiber of the minimal proper regular model of C when compared to a curve of reduction type $[I_0 - \mathcal{K} - (l-1)]$. We need the field to be global because for non-global one-dimensional function fields the quotient might not be finite. We have not been able to give a proof in the general case, but we can show the following:

Proposition 3.67. *If the residue characteristic is equal to 2, then Conjecture 3.66 holds.*

Proof. The proof follows from the proof of Lemma A.3, see Appendix A.8. The lemma is stated there for the situation

$$v(x_1) = 0,\ v(x_2) > 0,\ 0 \leq v(x_3) \leq 4l,$$

which implies $v(x_4) \leq \frac{1}{2}v(x_3)$. For every $Q \in J(k_v)$ let $x(Q)$ denote a set of integral Kummer coordinates for Q such that one of the $x(Q)_i$ is a unit. Then the proof of Lemma A.3 shows that we have $v(x(2^{n+1}P)_4) - v(x(2^nP)_4) \geq 2v(2)$ as long as $v(x(2^nP)_4) \geq 2v(2)$. The upper bound $2l$ for $v(x_4)$ implies that $v(x(2^lP)_4) = 0$ and thus $\varepsilon_v(2^lP)$ vanishes.

Using Appendix A.8 it is easy to see that the same principle applies as long as we have $v(x_3)v(x_4) > 0$ and $\mathcal{K} \neq I_0$. But if $v(x_3)v(x_4) = 0$, then we have $\varepsilon_v(P) = 0$ already, and so we are done. □

The proof suggests that if k is a number field and l is divisible by the ramification index e of k_v over $\mathbb{Q}_v$, then we might have $\varepsilon_v(p^{l/e}P) = 0$ for any

$P \in J_0(k_v)$ and indeed this was the case in our examples. However, since most of our experiments dealt with either $\mathbb{Q}_v$ or unramified extensions, we have not dared to include this into the statement of the conjecture. Anyway, for practical purposes – at least for our intended applications – Conjecture 3.66 does not seem to have much relevance. If $\mathcal{K} = I_0$, then there are several counterexamples to the statement of the conjecture.

Example 3.68. Let C be given by

$$y^2 = (x^2 + 1)(x^3 + p^6),$$

where $p > 2$ is a prime less than 100, and let $P = [(0, p^3) - \infty]$. Then we have $\varepsilon_v(nP) \neq 0$ for $n \in \{1, \ldots, 5\}$, but $\varepsilon_v(6P) = 0$.

Remark 3.69. According to Lemma 3.59 we cannot use Corollary 3.32 to bound the height constant. Yet if we can show that there are no $P \in J(k_v) \setminus J_0(k_v)$, then we get the bound

$$\beta_v \leq 2l,$$

which is certainly a significant improvement over the bound we get by applying Proposition 3.11. This condition is satisfied when $\mathcal{K} \in \{I_0, II, II^*\}$ and more generally when the Tamagawa number c_v is equal to 1.

3.6.5 Case (5)

In this case there is a cusp and a node in the reduction of C. If we explicitly construct the minimal proper regular model, we find that in the notation of Namikawa and Ueno it is of the form $[I_{m_1} - \mathcal{K} - l]$, where $\mathcal{K}$ is the Kodaira type of the elliptic curve E given by (3.26) and we have $l \geq 0$ and $m_1 > 0$. Note that the Kodaira type I_{m_1} is the reduction type of the elliptic curve E' with equation (3.27).

If $\mathrm{char}(\mathfrak{k}_v) \neq 2$, then we can find, using Hensel's Lemma, a factorisation

$$F(X, Z) = F_1(X, Z)G(X, Z)F_2(X, Z),$$

where

$$\tilde{F_1}(X, Z) = Z^2,\ \tilde{F_2}(X, Z) = X^3,\ \tilde{G}(X, Z) = X - Z,$$

and the valuation of the discriminant of G as well as the valuations of the resultants between the different forms vanish. In this case

$$v(\mathrm{disc}(F_1)) = m_1,\ v(\mathrm{disc}(F_2)) = m_2 > 0,$$

so that we have $v(\Delta) = m_1 + m_2$. Note that m_1 is the discriminant of the given equation of E' and m_2 is the discriminant of the given equation of E and this continues to hold for even residue characteristic.

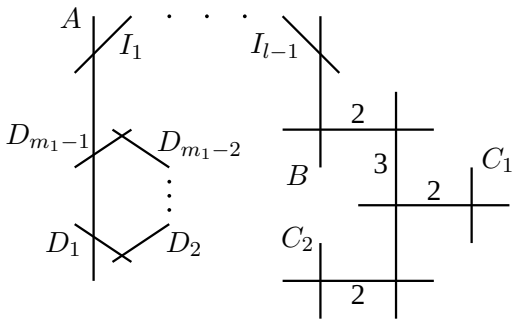

Figure 3.6: The special fiber of reduction type $[I_{m_1} - IV^* - l]$

We first suppose, similar to cases (1), (2) and (3) that we have

$$m_1 = \min\{v(f_6), 2v(f_5)\}.$$

In Remarks 3.44 and 3.45 it is explained in some detail how to find a transformation to reduce to this case; there is no additional difficulty in the present case as soon as we have computed m_1.

For now we assume that $\mathcal{K}$ is not multiplicative, which always holds when $l = 0$. Then we get from Proposition 1.37

$$\Phi_v \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathcal{G},$$

where

$$\mathcal{G} \in \{\{0\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}\}.$$

If $m_1 = 1$, then the special fiber is similar to the special fiber of type $[I_0 - \mathcal{K} - m]$, but now A is a genus 0 curve with a node. If $m_1 > 1$, then the special fiber $\mathcal{C}_v^{\min}$ again resembles the special fiber of type $[I_0 - \mathcal{K} - m]$, but now there is also an m_1-gon, with components $A = D_0, D_1, \ldots, D_{m_1-1}$. See Figure 3.6 for the case $\mathcal{K} = IV^*$.

As before, we denote the other components of multiplicity 1 in the part of the special fiber corresponding to $\mathcal{K}$, if any exist, by $C_1, \ldots, C_t$, where $t + 1 \in \{1, \ldots, 4\}$ is the number of components of K that have simple multiplicity.

We let

$$\begin{array}{rccc} \chi = (\chi_1, \chi_2) : J(k_v) & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathcal{G} \\ P & \mapsto & (i, j) \end{array}$$

denote the map induced by these numberings.

Similar to case (4) we have:

Lemma 3.70. *The curve C has a model of the form* (3.13) *whose closure $\mathcal{C}$ has rational singularities if and only if $l = 0$. If $l = 0$, then the given model already satisfies this condition.*

Proof. See the proof of Lemma 3.59. □

Thus we conclude that if $l > 0$, then ε_v does not factor through Φ_v in general, for the same reason as in case (4). Therefore we first deal with the case $l = 0$, which is of course the most common case in practice. This ensures that ε_v and μ_v factor through Φ_v. By the above discussion we know that for any point $P \in J(k_v)$ there is a multiple nP mapping to $[D_i - A]$, that is $\chi(nP) = (i, 0)$, where $1 \leq n \leq 4$ and $0 \leq i \leq m_1 - 1$.

It suffices to find a formula for $\mu_v(nP)$, since then we can compute $\hat{\lambda}_v(P)$ from $\hat{\lambda}_v(nP)$ using Proposition 3.23. We find such a formula upon noticing that points satisfying $\chi(P) = (i, 0)$ where $i \neq 0$ (the other case is trivial), are characterised by

$$v(x_1) > 0, v(x_2) \geq 0, v(x_3) = 0, v(x_4) > 0.$$

As in (3.24) we define

$$w(P) := \min\{v(x_1), v(x_4), m_1/2\}$$

and the following lemma is proved similarly to Lemma 3.46. In fact, most of the difficulties in that proof disappear, so the proof is even easier and is omitted.

Lemma 3.71. *If $\chi_2(P) = 0$, then we have*

$$\varepsilon_v(P) = 2\min\{\chi_1(P), m_1 - \chi_1(P)\}.$$

The proof of the next lemma is also a simpler version of the proof of Lemma 3.47.

Lemma 3.72. *Suppose $\chi_2(P) = 0$. Then we have*

$$\varepsilon_v(P) = 2w(P),$$

so in particular

$$w(P) = \min\{\chi_1(P), m_1 - \chi_1(P)\}.$$

The last two results can be combined into a proof of the following proposition, which is the same as the proof of Proposition 3.49.

Proposition 3.73. *If $\chi_2(P) = 0$, then we have the formula*

$$\mu_v(P) = \frac{w(P)(m_1 - w(P))}{m_1}.$$

As in case (4), the situation $l > 0$ is considerably more complicated. We prove a formula for points satisfying $\chi(P) = (i, 0)$, where $0 \leq i \leq m_1 - 1$. If $\mathcal{K}$ is not multiplicative, then we can find some $n \leq 4$ such that nP satisfies this for all $P \in J(k_v)$; otherwise, n might be larger. For a point $P \in J(k_v)$ we define

$$w_1(P) := \min\{v(x_1), v(x_4), m_1/2\}$$

and

$$w_2(P) := \min\{v(x_3), v(x_4), 2l\}.$$

Theorem 3.74. *Suppose C has reduction type $[I_{m_1} - \mathcal{K} - l]$, where $\mathcal{K}$ is a Kodaira type, $m_1, l \geq 0$. Suppose that $v(f_0) \geq 6l, v(f_1) \geq 4l, v(f_2) \geq 2l$, $v(f_6) \neq 2v(f_5)$ and that applying Tate's algorithm to E yields no transformations except for $(\xi, \eta) \mapsto (\pi^{-2l}\xi, \pi^{-3l}\eta)$. Let $x = (x_1, x_2, x_3, x_4)$ be a set of v-integral Kummer coordinates for $P \in J(k_v)$ satisfying $\chi_2(P) = 0$ such that $v(x_j) = 0$ for some j. Then we have*

$$\mu_v(P) = \frac{w_1(P)(m_1 - w_1(P))}{m_1} + w_2(P).$$

Proof. See Appendix A.9. □

Using the preceding theorem, we can compute $\mu_v(nP)$ for all possible reduction types $\mathcal{K}$, where either $n \in \{1, \ldots, 4\}$ or $n = m_2 \geq 1$ when $\mathcal{K}$ is multiplicative. We might have to apply some transformations, but using the behavior of the canonical local height under changes of the model we can compute $\mu_v(nP)$ on the original model. It is not hard to find n from the valuations of the discriminant Δ and the valuations of the coefficients of F and H. We could also state an analog of Conjecture 3.66 in case (5) and prove it for residue characteristic 2 as in Proposition 3.67.

It is unfortunate that we have $n > 4$ for $[I_{m_1} - I_{m_2} - l]$ and $m_1, m_2 > 4$. At least we can always use a transformation to ensure that $m_2 \leq m_1$. However, this reduction type should hardly ever occur in practice, because if it does, the valuation of $\Delta(C)$ must be at least 22.

Remark 3.75. Let k be a one-dimensional function field that is not a global field and let $v \in M_k$. Then the formulas for cases (1) to (5) show that in cases (1), (2) and (3), that is in the semistable cases, the group U_v of points which ε_v vanishes on has finite index in $J(k_v)$, see Remark 3.10. In cases (4) and (5) this may not be true and we have not dared to extend Conjecture 3.66 to Jacobians defined over such fields. However, our methods for the computation of μ_v work perfectly well in such cases, in contrast with the original method due to Flynn and Smart which is not guaranteed to work even theoretically.

Remark 3.76. In case (5) we can only use Corollary 3.32 to bound the height constant β_v in special situations, even if we assume $l = 0$. For instance, if

$m_1 = 1$, we can proceed as in Remark 3.60. However, the results of this section are most useful for bounding β_v when we have $c_v(E) = 1$, see Remark 3.69. Whenever this is satisfied (so for instance when $\mathcal{K} \in \{I_0, II, II^*\}$) we can conclude

$$\begin{aligned} m_1 \text{ even} \quad &\Rightarrow \quad \beta_v \leq \frac{m_1}{4} + 2l, \\ m_1 \text{ odd} \quad &\Rightarrow \quad \beta_v \leq \frac{m_1^2 - 1}{4m_1} + 2l. \end{aligned}$$

3.7 Archimedean places

Recall from Section 2.4 that in the case of elliptic curves there are essentially three methods available for the computation of archimedean canonical local heights, namely Tate's series, theta (more precisely, Weierstrass σ-) functions and the isogeny trick due to Bost and Mestre. We exhibit analogs of all three of these methods in the case of Jacobian surfaces. Surprisingly, the analog of Tate's series turns out to be the most efficient.

The setup is a smooth projective curve C of genus 2, given by an equation of the form (3.13) with Jacobian J and Kummer surface K, defined over a number field k. We want to compute the canonical local height $\hat{\lambda}_v(x)$ for an archimedean place v and a set of Kummer coordinates x on K.

3.7.1 Approximating μ_v using a truncated series

The first method was already introduced in Section 3.2.2 and is due to Flynn and Smart, see [43]. It uses the definition (3.22) of $\hat{\lambda}_v$: For a given desired accuracy, we need a bound on the number of summands of μ_v needed to compute $\hat{\lambda}_v$ to that accuracy; such a bound can be found using a bound on the local height constant γ_v, see the discussions at the end of Section 3.2.2 and Section 3.2.3. Because we can use floating point arithmetic, the repeated applications of δ are not so expensive. Moreover, we can renormalize our set of Kummer coordinates at each step, thus guaranteeing convergence. In order to use the height constant, we transform the model of C to get a simplified model satisfying $H = 0$ and then use Corollary 3.25.

However, the height constant bound at an archimedean place may not be sharp, see the discussion in [92, §9], so there is room for improvement if one could improve on this bound. Some results in this direction were obtained by Uchida in [103, §6] who uses an optimization approach with constraints. One has to be careful though, because his algorithm is similar to a method already used by Flynn and Smart which yielded some bounds that were much too small, see the discussion in [92, §9]. Of course any improvement, such as Uchida's, is of independent interest.

Furthermore, there are numerical problems, namely one has the usual problem of rounding errors. In addition, applying δ to a (floating point approximation of a) set of coordinates x may result in $\delta(x)$ not representing a point on K anymore, so one has to adjust the coordinates, for example by fixing any three of the coordinates and choosing the fourth coordinate to satisfy the Kummer surface equation up to a prescribed accuracy. Since the equation is quadratic in x_4 and quartic in the other x_i, fixing the first three coordinates is usually the best choice.

Another conceivable method would be the following: First compute a bound for the absolute value of the gradient of $\varepsilon_v(P)$ and hence of $\mu_v(P)$, then find a torsion point Q sufficiently close to P such that we can compute $\mu_v(Q)$ in order to approximate $\mu_v(P)$ to the desired accuracy. The problem is how to find such a Q. This is easy if we use complex uniformisation, but this approach is not very efficient, see below. We could restrict to 2^m-torsion and use repeated halving of the image of the point on K (as in [92, §5]), but this is slower than the algorithm that we have already discussed.

3.7.2 Theta functions

The second method discussed in Section 2.4 uses the original description of archimedean Néron functions due to Néron given in Proposition 1.39. Suppose that our curve C is embedded into $\mathbb{P}^2_{\mathbb{C}}$ using v. By virtue of Corollary 3.25 we can assume that C is given by a model of the form $Y^2 = F(X,1)$, where $\deg(F(X,1)) = 5$. Let J be the Jacobian of C and Θ the theta divisor corresponding to the Abel-Jacobi map embedding C into J with base point ∞, so the divisor D_1 that our embedding of the Kummer surface corresponds to is equal to 2Θ. Recall the notation from Section 1.6: We let $\tau_v \in \mathfrak{h}_2$ such that $J(\mathbb{C})$ is isomorphic to $\mathbb{C}^2/\Lambda_v$, where $\Lambda_v = \mathbb{Z}^2 \oplus \tau_v\mathbb{Z}^2$. We define the map j by

$$j : \mathbb{C}^2 \longrightarrow\!\!\!\!\!\rightarrow \mathbb{C}^2/\Lambda_v \xrightarrow{\cong} J(\mathbb{C}).$$

Finally, let $a = (1/2, 1/2), b = (1, 1/2) \in \mathbb{C}^2$ and let $\theta_{a,b}$ denote the theta function with characteristic $[a; b]$ defined in Section 1.6.

Proposition 3.77. *(Pazuki) The function $\theta_{a,b}$ has divisor $j^*(\Theta)$. Moreover, the following function is a Néron function associated with Θ and v*

$$\hat{\lambda}'_{\Theta,v}(P) = -\log|\theta_{a,b}(z(P))|_v + \pi \operatorname{Im}(z(P))^T (\operatorname{Im}(\tau_v))^{-1} \operatorname{Im}(z(P)),$$

where $j(z(P)) = P$.

Proof. This was stated without proof by Pazuki in [80, Proposition 3.1], but it is in fact rather easy to verify: It is a classical theorem (see [59,

Chapter 13, Theorem 4.1]) that the divisor of the Riemann theta function $\theta = \theta_{0,0}$ is a translate by a point w of the usual theta divisor and that $2w$ is the image on J of the canonical class on C. Using this it is not hard to see that the odd function $\theta_{a,b}$ has divisor $j^*(\Theta)$. Then one uses Proposition 1.39 and Remark 1.41 to find an expression of a Néron function in terms of the normalized theta function $\theta'_{a,b}$; the right hand side in Proposition 3.77 is equal to this expression after a straightforward manipulation.

Alternatively one can show directly that $\hat{\lambda}'_{\Theta,v}$ satisfies the properties of a Néron function. □

We can use this proposition to compute the function $\hat{\lambda}_v(x)$, where x is a set of Kummer coordinates for a point $P \in J(k)$. Suppose that $P \notin \mathrm{supp}(\Theta)$, that is $\kappa_1(P) \neq 0$. We actually compute $\hat{\lambda}_{1,v}(P) = \hat{\lambda}_v(x'(P))$, where $x'(P)_i = \kappa(P)_i/\kappa(P)_1$. Because both $2\hat{\lambda}'_{\Theta,v}$ and $\hat{\lambda}_{1,v}$ are Néron functions associated with 2Θ and v, there exists some constant d_v satisfying

$$\hat{\lambda}_{1,v}(P) = 2\hat{\lambda}'_{\Theta,v}(P) + d_v$$

for all $P \in J(\mathbb{C}) \setminus \mathrm{supp}(\Theta)$ (see also [80, Proposition 4.1]). This constant can be calculated easily as follows: We first find $z \in \mathbb{C}^2$ such that $3z \in \Lambda$. Then there is some $Q \in J(\mathbb{C})[3]$ such that $j(z) = Q$. We find this Q and by [80, Proposition 4.2] we have $Q \notin \mathrm{supp}(\Theta)$. Hence we obtain

$$d_v = \hat{\lambda}_{1,v}(Q) - 2\hat{\lambda}'_{\Theta,v}(Q) = v(x'(Q)) - \varepsilon_v(Q)/3 - 2\hat{\lambda}'_{\Theta,v}(Q). \qquad (3.31)$$

Once we have found d_v, we can compute $\hat{\lambda}_v(x)$ for any set of Kummer coordinates for a point $P \in J(k)$ satisfying $\kappa_1(P) \neq 0$. If this condition is not satisfied, we can either apply transformations in order to move the point or we can use the canonical local height for a suitable different divisor in the class of 2Θ; the constant d_v is different in this case and has to be recomputed.

Recall that for real places v the corresponding method for elliptic curves is quite efficient, because there are several computational tricks available. It is possible – and implemented for example in `Magma` by van Wamelen – to go back and forth between the algebraic Jacobian J and the analytic Jacobian $\mathbb{C}^2/\Lambda_v$ and to compute theta functions. One can use Richelot isogenies to construct a very quick algorithm to compute the period matrix, cf. [11] and it should also be possible to speed up the computation of theta functions using computational tricks similar to [23, Algorithm 7.5.7].

The problem is that we do not have a fast method for computing complex coordinates of points on Jacobian surfaces. For elliptic curves we have already mentioned a method commonly called Landen's transformation (see [23, Algorithm 7.4.8]) that gives a rapid algorithm for this problem, but it seems to have no 2-dimensional analog. If such an analog were found, then the approach described in this section could become quite competitive, but

at the moment it is inferior in practice to the series approximation of μ_v. Its advantage is that it can be generalized quite easily to the higher genus situation, because Proposition 3.77 generalizes, see Proposition 4.15 below.

Finally it should be mentioned that Silverman has found a bound on the local height constant for archimedean valuations in the case of elliptic curves in [88] using the complex uniformisation and Proposition 2.18. This bound is sometimes better than the bound one gets from applying other techniques, see [28]. In the present situation one could try to emulate this and bound the difference between the archimedean canonical local height $\hat{\lambda}_v(P)$ and $2\hat{\lambda'}_{\Theta,v}(P) + d_v$, possibly using techniques similar to [80], where a lower bound for $\hat{\lambda'}_{\Theta,v}$ is found. We have not attempted this, but it appears to be a promising direction for future research.

3.7.3 Richelot isogenies

Suppose that the embedding corresponding to v is real and view C as embedded into the real projective plane using v, given by an equation satisfying $H = 0$. Moreover suppose that all the roots of $F(X, 1)$ are real. Bost and Mestre show in [11] how to construct a sequence of maps $\phi_{n-1} : C_n \longrightarrow C_{n-1}$ on genus 2 curves $C_n : Y^2 = f_n(X)$, where $C_0 = C$ and $f_0(X) = F(X, 1)$, that deform C into a singular curve with 3 nodes. The roots of the polynomials f_n converge quadratically to the x-coordinates of these points and this approach provides a quick method for the computation of the period matrix τ_v.

The maps ϕ_n induce isogenies on the corresponding Jacobians, which are called Richelot isogenies. See [20, Chapter 9] for a more general account of these classical maps. Flynn has found explicit formulas for the induced maps on the Kummer surface in [42], so it seems quite promising to use these formulas for an analog of the isogeny method of Bost and Mestre described in Section 2.4, since we know from Proposition 3.24 how the canonical local height changes under isogenies.

Suppose that $P_0 \in J(\mathbb{R})$ lies on the connected component of the identity (otherwise there might be no real preimage of P_0 under ϕ_0) and $(P_n)_n$ is the sequence of points defined by $P_{n-1} = \phi_n(P_n)$. We suppose $\kappa_i(P_n) \neq 0$ for all n, so that we can use $\hat{\lambda}_{i,v}$, since we need a canonical local height associated with some divisor – the sequence of canonical local heights on Kummer coordinates does not converge, unless we use a consistent normalization.

This is problematic, but what is worse is that the sequence of canonical local heights $(\hat{\lambda}_{D_i,v}(P_n))_n$ only converges linearly with convergence factor 2, coming from Proposition 3.24 and the fact that the roots of the f_n converge quadratically. So this is slower than the series approach which has convergence factor 4; moreover finding the preimage of a set of Kummer coordinate using Flynn's formulas involves computing inverses of 4×4 matrices

and several square roots and is thus slower in general than an application of δ.

Chapter 4

Jacobian threefolds

4.1 Embedding the Kummer variety

Let l denote a field of characteristic $\mathrm{char}(l) \neq 2$. In order to generalize the results from the previous chapter we need to find an embedding of the Kummer variety associated to the Jacobian of a smooth projective curve of genus 3 into projective space of dimension $2^g - 1 = 7$. Since not all those curves are hyperelliptic, we first restrict to those which are. This is reasonable because all genus 2 curves are hyperelliptic and so we expect that the results for Jacobian surfaces generalize more easily to Jacobians of other hyperelliptic curves.

Since the genus is odd there is another complication that we have not encountered so far. Recall that in Sections 3.1 and 3.3 we constructed the Kummer surface by finding an embedding using the fact that generic points of the Jacobian J of a smooth projective genus 2 curve C are represented by divisors of the form

$$(P_1) + (P_2) - 2(\infty)$$

or

$$(P_1) + (P_2) - ((\infty^+) + (\infty^-)),$$

where $P_1, P_2 \in C$, depending on whether there exists a unique point at infinity or not. Therefore generic points on the Jacobian can be represented using unordered pairs of points on the curve.

In the present situation, we have an analogous result if C is a smooth projective genus 3 curve over l with Jacobian J and an l-rational Weierstrass point, which we can assume to be at infinity. Then we can find a representative of the form

$$(P_1) + (P_2) + (P_3) - 3(\infty), \tag{4.1}$$

where $P_1, P_2, P_3 \in C$ and this representation is unique for generic points on J. Here generic means that if we have a representation (4.1), then $P_i \neq \infty$ and we have $P_i \neq P_j^-$ for all distinct $i, j \in \{1, 2, 3\}$, where $Q \mapsto Q^-$ denotes the hyperelliptic involution on C.

However, in the complementary case we have to consider representatives of the form

$$(P_1) + (P_2) + (P_3) + (P_4) - 2((\infty^+) + (\infty^-)),$$

and these are not unique, even for generic points. In this more general situation there exists a different approach due to Stoll, see [99], which also contains some ideas for the embedding of the Kummer threefold in the non-hyperelliptic case.

Therefore we first restrict to curves having an l-rational Weierstrass point at infinity. Consider an affine equation of the form

$$Y^2 = F(X, 1) \tag{4.2}$$

where

$$F(X,Z) = f_0Z^8+f_1XZ^7+f_2X^2Z^6+f_3X^3Z^5+f_4X^4Z^4+f_5X^5Z^3+f_6X^6Z^2+f_7X^7Z \tag{4.3}$$

is a binary octic form in $l[X,Z]$ without multiple factors with $\deg(F(X,1)) = 7$. Let C denote the hyperelliptic curve of genus 3 given by the smooth projective model of (4.2). Let J be the Jacobian of C. An embedding of the Kummer variety $K = J/\{\pm 1\}$ of J can be given by a basis of $\mathcal{L}(2\Theta)$; such a basis has been found by Stubbs in [100] and we reproduce it here. Suppose we have a generic point, where for the remainder of this section *generic* means that P is represented by an unordered triple of affine points $(x_1,y_1),(x_2,y_2),(x_3,y_3) \in C$, where all x_i are pairwise distinct. An embedding of the Kummer threefold is given by

$$\kappa(P) = (\kappa_1(P),\ldots,\kappa_8(P)),$$

where the functions $\kappa_1,\ldots,\kappa_8$ are given by

$$\begin{aligned}
\kappa_1 &= 1,\\
\kappa_2 &= x_1+x_2+x_3,\\
\kappa_3 &= x_1x_2+x_1x_3+x_2x_3,\\
\kappa_4 &= x_1x_2x_3,\\
\kappa_5 &= b_0^2 - f_7\kappa_2^3 + f_7\kappa_3\kappa_2 - f_6\kappa_2^2 + 3f_7\kappa_4 + 2f_6\kappa_3,\\
\kappa_6 &= \kappa_2b_0^2 + 2b_0b_1 - f_7\kappa_2^4 + 3f_7\kappa_3\kappa_2^2 - f_6\kappa_2^3 - f_7\kappa_3^2 - f_7\kappa_4\kappa_2 + 2f_6\kappa_3\kappa_2\\
&\quad -f_5\kappa_2^2 + 2f_5\kappa_3,\\
\kappa_7 &= b_1^2 - \kappa_3b_0^2 + f_7\kappa_3\kappa_2^3 - 2f_7\kappa_3^2\kappa_2 + f_6\kappa_3\kappa_2^2 + f_7\kappa_4\kappa_3 - f_6\kappa_3^2 + f_5\kappa_3\kappa_2\\
&\quad -3f_5\kappa_4,\\
\kappa_8 &= \kappa_2b_1^2 + 2\kappa_3b_0b_1 + \kappa_4b_0^2 + f_7\kappa_3^2\kappa_2^2 - f_7\kappa_2^3\kappa_4 + f_7\kappa_2\kappa_3\kappa_4 - f_7\kappa_3^3\\
&\quad +f_6\kappa_3^2\kappa_2 - f_6\kappa_4\kappa_2^2 + f_5\kappa_3^2 - f_5\kappa_4\kappa_2.
\end{aligned}$$

Here we have

$$\begin{aligned}
b_0 &= (x_1y_2 - x_2y_1 - x_3y_2 + x_3y_1 - x_1y_3 + x_2y_3)/d,\\
b_1 &= (x_3^2y_2 - x_3^2y_1 + x_2^2y_1 + y_3x_1^2 - y_2x_1^2 - y_3x_2^2)/d,\\
d &= (x_1-x_2)(x_1-x_3)(x_2-x_3).
\end{aligned}$$

We also provide formulas for the values of $\kappa(P)$ when P is not of the form considered above, because apparently they do not exist in the literature. For this we first notice that in the generic case b_0 and b_1 satisfy that

$$B(X,Z) = b_2Z^4 + b_1XZ^3 + b_0X^2Z^2 \tag{4.4}$$

for some $b_2 \in l$, where the Mumford representation of P is

$$(A(X,Z), Y - B(X,Z)),$$

see the discussion in Section 5.2.2. We can use this observation for our generalization of κ. If P still has a unique representative of the form (4.1), where now at least two of the x_i are equal, then the formulas for κ remain valid if b_0 and b_1 are not given by the explicit formulas above, but rather as coefficients of $B(X,Z)$ as in (4.4).

In order to find formulas when P has a unique representative of the form

$$((x_1,y_1)) + ((x_2,y_2)) - 2(\infty)$$

we first assume that P is generic and satisfies $x_1x_2x_3 \neq 0$ and write the κ_i in terms of $(w_1,z_1),(w_2,z_2),(w_3,z_3)$, where $z_j = 1/x_j$ and $w_j = y_j/x_j$. We then multiply by the common denominator and set $w_3 = 0$. Assuming $x_1 \neq x_2$ we find

$$\begin{aligned}
\kappa_1 &= 0,\\
\kappa_2 &= 1,\\
\kappa_3 &= x_1 + x_2,\\
\kappa_4 &= x_1x_2,\\
\kappa_5 &= f_5 + 2f_6\kappa_3 + f_7\kappa_3^2 + 2\kappa_4 f_7,\\
\kappa_6 &= f_4 + f_5\kappa_3 - \kappa_4 f_7\kappa_3,\\
\kappa_7 &= -f_4\kappa_3 - 3\kappa_4 f_5 + \kappa_4^2 f_7,\\
\kappa_8 &= (f_3\kappa_3^3 + f_1\kappa_3 + f_2\kappa_3^2 + 2f_0 - 2y_1y_2 + \kappa_4 f_4\kappa_3^2 - 3\kappa_4 f_3\kappa_3 - 2\kappa_4 f_2\\
&\quad +\kappa_4^2 f_5\kappa_3 - 2\kappa_4^2 f_4 + \kappa_4^3 f_7\kappa_3 + 2\kappa_4^3 f_6)/(x_1 - x_2)^2.
\end{aligned}$$

For the case $x_1 = x_2$ it suffices to use the same $\kappa_1,\ldots,\kappa_7$ and

$$\kappa_8 = b_1^2 - (\kappa_4 - \kappa_3^2)(-2\kappa_4 f_7\kappa_3 - \kappa_4 f_6 + f_7\kappa_3^3 + \kappa_3^2 f_6 + f_5\kappa_3 + f_4),$$

where b_1 is as in (4.4).

Now consider points represented by

$$((x_1,y_1)) - (\infty).$$

We first look at quotients of the form $\kappa_i(P)/\kappa_5(P)$, where P is again assumed generic, and then take the limit $(x_2,y_2) \to (x_3,-y_3)$.The result is

$$\kappa(P) = (0,0,0,0,1,-x_1,x_1^2,x_1^3).$$

A similar argument shows that we have

$$\kappa(0) = (0,0,0,0,0,0,0,1).$$

4.2 Defining equations for the Kummer variety

As we have seen in the previous chapter, the Kummer surface associated to a Jacobian surface can be embedded as a quartic hypersurface into $\mathbb{P}^3$. It turns out that the defining equations for the Kummer threefold are far more complicated, but at least we can still describe them explicitly.

Proposition 4.1. *Let K denote the Kummer variety of a Jacobian of dimension $g \geq 2$, with embedding $\kappa = (\kappa_1, \ldots, \kappa_{2^g})$ into $\mathbb{P}^{2^g-1}$. Then the image of K under κ can be described as an intersection of quartics.*

Proof. This proof was suggested to me by Tzanko Matev. Let $\mathcal{Q}$ denote the set of monic quadratic monomials in the κ_i and let $d \leq m$ denote the dimension of the space they generate, where $m = \binom{2^g+1}{2}$ is the cardinality of $\mathcal{Q}$. Let $\mathcal{S} = \{s_1, \ldots, s_d\}$ be a subset of $\mathcal{Q}$ that is linearly independent in $\mathbb{Q}(f_0, \ldots, f_7)[q_1, \ldots, q_m]$, where the elements of $\mathcal{Q}$ are ordered so that we have $\mathcal{Q} = \{q_1, \ldots, q_m\}$ with $q_i = s_i$ for $i = 1, \ldots, d$.

Let α denote the 2-uple embedding of $\mathbb{P}^{2^g-1}$ into $\mathbb{P}^{m-1}$ such that if $P \in J$, then we have

$$\alpha_i(\kappa(P)) = q_i(P) \quad \text{for all } i \in \{1, \ldots, m\}.$$

Then there are $m - d$ linear relations on the image of $K = \kappa(J)$ under α. Now consider an embedding $\beta : J \hookrightarrow \mathbb{P}^{4^g-1}$ given by a basis of $\mathcal{L}(4\Theta)$ whose first d elements are equal to $s_1, \ldots, s_d$. Then we have a commutative diagram

$$\begin{array}{ccc} J & \xrightarrow{\beta} & \mathbb{P}^{4^g-1} \\ {\scriptstyle\kappa}\downarrow & & \downarrow{\scriptstyle\gamma} \\ \mathbb{P}^{2^g-1} & \xrightarrow[\alpha]{} & \mathbb{P}^{m-1} \end{array}$$

where γ is a rational map defined as follows: If $z = (z_1, \ldots, z_{4^g})$, then $\gamma(z) = y$, where $y_i = z_i$ for $i = 1, \ldots, d$ and the other y_i are determined by the linear relations of $\mathcal{Q}$. By construction, we have that $\beta(J)$ lies in the domain of γ and in fact

$$\gamma(\beta(J)) \cong \alpha(\kappa(J)).$$

But it follows from [6, Theorem 7.4.1] that the image of J under β is defined by an intersection of quadrics, which then must hold for $\gamma(\beta(J))$ as well, since γ has degree 1. As the pullback under α of $\gamma(\beta(J))$ is isomorphic to K, the result follows. □

Hence it suffices to find a basis for the space of quartic relations on K to describe K. We first compute a lower bound on the dimension of this space.

n	$m(n)$	$e(n)$	$d(n)$
1	4	4	4
2	10	10	10
3	20	20	20
4	35	34	34

Table 4.1: Dimensions in genus 2

n	$m(n)$	$e(n)$	$d(n)$
1	8	8	8
2	36	36	35
3	120	112	≤ 112
4	330	260	≤ 260

Table 4.2: Dimensions in genus 3

For $n \geq 1$ let $m(n)$ denote the number of monic monomials of degree n in $\kappa_1, \ldots, \kappa_{2g}$ and let $d(n)$ denote the dimension of the space spanned by them. Then we have $m(n) = \binom{2g+n-1}{n}$. Moreover, let $e(n)$ denote the dimension of the space of even functions in $\mathcal{L}(2n\Theta)$. By [6, Corollary 4.7.7] this is equal to $(2n)^g/2 + 2^{g-1}$. Since a monomial of degree n in the κ_i induces an even function in $\mathcal{L}(2n\Theta)$, we always have $d(n) \leq e(n)$.

In genus 2, the dimension count is given in Table 4.1. We know that $d(4)$ can be at most $e(4) = 34$, and indeed the space of quadratic relations in the κ_i is one-dimensional, spanned by the Kummer surface equation (3.11).

Now we return to the case of genus 3. Stubbs has found the following quadratic relation between the κ_i and shown that it is unique up to scalars:

$$R_1 : \kappa_1\kappa_8 - \kappa_2\kappa_7 - \kappa_3\kappa_6 - \kappa_4\kappa_5 - 2f_5\kappa_2\kappa_4 + f_5\kappa_3^2 + 2f_6\kappa_3\kappa_4 + 3f_7\kappa_4^2 = 0 \quad (4.5)$$

The dimensions for genus 3 are presented in Table 4.2. The existence and uniqueness of R_1 implies that $d(2) = 35$, but since $e(2) = 36$, this means that there is an element of $\mathcal{L}(4\Theta)$ not coming from a quadratic monomial in the κ_i, which does not happen in genus 2. Accordingly, we can at this point only bound $d(3)$ and $d(4)$ from above. It follows that in genus 3 there must be at least $70 = 330 - 260$ quartic relations on the Kummer variety. But 36 of these are multiples of the quadratic relation R_1, so there must be at least 34 genuine quartic relations.

In [100, Chapter 5] Stubbs lists, in addition to R_1, 26 quartic relations and conjectures that these 27 relations are independent and form a basis of the space of all relations on the Kummer variety. These are the relations that are at most quadratic in $\kappa_5, \ldots, \kappa_8$. He was not able to prove either of these conjectures. Using current computing facilities we can verify the former conjecture quite easily, but because of our dimension counting argument, we know that the latter conjecture cannot be correct.

	x	y
x_i	1	0
y_i	0	1
f_i	$-i$	2
$\kappa_i, i \leq 4$	$i-1$	0
$\kappa_i, i > 4$	$i-9$	2

Table 4.3: x- and y-weight

How can such relations be derived? We employ the technique used already by Stubbs to find his relations to obtain a complete system of defining equations. Because of the enormous size of the algebra involved in these computations, we cannot simply search for relations among all monomials. Instead we split the monomials into parts of equal x-weight and y-weight. These are homogeneous weights discussed in [100, §3.5] that were already used by Flynn in [40] in order to derive quadratic relations defining a Jacobian surface in $\mathbb{P}^{15}$. See Table 4.3, reproduced essentially from [100, Figure 3.4].

On monomials of equal x- and y-weight we can use linear algebra to find relations; we continue this process with increasing weights until we have found enough quartic relations to generate a space of dimension 70. The difficulty of this increases mostly with the y-weight, the x-weight is not so important.

Theorem 4.2. *There are relations $R_2, \ldots, R_{35}$ which can be downloaded from the author's homepage [74] such that the space of relations of degree at most 4 in $(\kappa_1, \ldots, \kappa_8)$ is generated by $R_1, \ldots R_{35}$ and the largest y-weight of the R_i is 8.*

Proof. Using a computer algebra system, for instance `Magma`, one can check that $R_1, \ldots, R_{35}$ are indeed relations on K and that they are independent. For the latter it suffices to check that the space

$$W = \{R_2, \ldots, R_{35}\} \cup \{\kappa_i \kappa_j R_1 : 1 \leq i \leq j \leq 8\}$$

has dimension equal to 70 for one example, say for $F(X, Z) = Z^8 + X^7 Z$. For this example, we can also compute all quartic relations and check that the space they generate has dimension 70 and equals W. It now follows that the space of all quartic relations has dimension exactly 70 in general and we are done. □

Corollary 4.3. *The relations on the Kummer threefold are generated by the relations $R_1, \ldots, R_{35}$.*

Proof. Combine Proposition 4.1 with Theorem 4.2. □

Next we generalize a useful notion from Chapter 3, namely that of Kummer coordinates.

Definition 4.4. Let l be a field of characteristic different from 2 with algebraic closure $\bar{l}$ and let $x = (x_1, \ldots, x_8) \in \mathbb{A}^8_{\bar{l}} \setminus \{(0, \ldots, 0)\}$. Let $K \subset \mathbb{P}^7_l$ be the Kummer variety associated with the Jacobian J of a smooth projective genus 3 curve defined over l. We say that x is a *set of Kummer coordinates on* K if the image of x in $\mathbb{P}^7_{\bar{l}}$ lies on K. If $P \in J$, then we say that x is a *set of Kummer coordinates for* P if x represents $\kappa(P)$, that is, if $\kappa(P) = (x_1 : \ldots : x_8)$. The set of all sets of Kummer coordinates on K is defined by

$$K_{\mathbb{A}} := \{(x_1, \ldots, x_8) \in \mathbb{A}^8 : \exists P \in K \text{ such that } P = (x_1 : \ldots : x_8)\}.$$

4.3 Remnants of the group law

In Chapter 3 we used the Kummer surface in order to define and compute canonical heights. In the process we repeatedly used the fact that the group law on the Jacobian is reflected on the Kummer surface. Theoretically the same holds in genus 3, but some new problems arise as we shall see in this section.

We let l denote a field of characteristic $\mathrm{char}(l) \neq 2$. As before, we let J be the Jacobian of a smooth projective curve C of genus 3 defined over l, given by a model (4.2). Let K be the Kummer threefold associated to J that we have constructed in the previous sections. Let $T \in J[2]$; then Duquesne has found a matrix W_T in [32] such that projectively the identity

$$\kappa(P + T) = W_T \kappa(P)$$

holds for all $P \in J$. It follows from general theory that such a matrix must exist as in the genus 2 case and Duquesne's method of finding it is analogous to the method employed by Flynn in [41] and used by us in Section 3.3.4 in the case of genus 2 and $\mathrm{char}(l) = 2$, although there are a few additional technical difficulties. We also have that if $T \in J(l)[2]$, then the entries of W_T are l-rational.

Now let $P, Q \in J$. Then we know that in general $\kappa(P + Q)$ and $\kappa(P - Q)$ cannot be found from $\kappa(P)$ and $\kappa(Q)$, but the unordered pair $\{\kappa(P + Q), \kappa(P - Q)\}$ can be. In fact, in the analogous situation in genus 2 there are biquadratic forms $B_{ij} \in l[x_1, \ldots, x_4; y_1, \ldots, y_4]_{2,2}$ such that if x and y are Kummer coordinates for P and Q, respectively, then there are Kummer coordinates w, z for $\kappa(P + Q), \kappa(P - Q)$, respectively, such that

$$w * z = B(x, y) \tag{4.6}$$

holds for all i, j and these were found in the general case in Section 3.3.3. Recall that (4.6) is an abbreviation for

$$\begin{aligned} B_{ij}(x,y) &= w_i z_j + w_j z_i \text{ for } i \neq j \\ B_{ii}(x,y) &= w_i z_i. \end{aligned}$$

We want to find such forms for $g = 3$. Unfortunately the following result says that they cannot exist in general.

Proposition 4.5. *Let J be the Jacobian of a smooth projective hyperelliptic curve C of genus 3, given by a model (4.2), and let K be the Kummer threefold associated to J. There are no biquadratic forms $B_{ij}(x,y)$, where $1 \leq i, j \leq 8$, satisfying the following: If x and y are sets of Kummer coordinates for $P, Q \in J$, respectively, then there are Kummer coordinates w, z for $P+Q, P-Q$, respectively, such that (4.6) holds.*

Proof. We can work geometrically, so we assume l is algebraically closed. Suppose such forms $B_{ij}(x,y)$ exist. Let us fix Kummer coordinates $x(T) = (x(T)_1, \ldots, x(T)_8)$ for all $T \in J[2]$.

For each $T \in J[2]$ we get a map

$$\pi_T : l[x_1, \ldots, x_8; y_1, \ldots, y_8] \longrightarrow l[y_1, \ldots, y_8],$$

given by evaluating the tuple x at $x(T)$. This induces a map

$$\pi_T : \frac{l[x_1, \ldots, x_8; y_1, \ldots, y_8]_{2,2}}{(R_1(x), R_1(y))} \longrightarrow \frac{l[y_1, \ldots, y_8]_2}{(R_1(y))}.$$

Now consider

$$R_1(B) := B_{18} - B_{27} - B_{36} - B_{45} - 2f_5 B_{24} + 2f_5 B_{33} + 2f_6 B_{34} + 6f_7 B_{44} \quad (4.7)$$

and let $\overline{R_1(B)}$ denote the image of $R_1(B)$ in $\frac{l[x_1,\ldots,x_8;y_1,\ldots,y_8]_{2,2}}{(R_1(x),R_1(y))}$. Then we must have

$$\pi_T(\overline{R_1(B)}) = 0 \quad \text{for all } T \in J[2]. \quad (4.8)$$

This follows from (4.5), since if $B(x(T), y) = w * z$, where y is a set of Kummer coordinates for some $P \in J$, then w and z are both Kummer coordinates for $P + T = P - T$ and thus we have $B_{i,j}(x(T), y) = 2z_i z_j$ for $1 \leq i \neq j \leq 8$ and $B_{i,i}(x(T), y) = z_i^2$ for $i \in \{1, \ldots, 8\}$, if $x(T$ and y the coordinates are scaled suitably so that $z = w$. But z must satisfy (4.5).

We claim that $\overline{R_1(B)}$ itself vanishes. In order to show this we fix $T \in J[2]$ and let

$$S(T) = \{s_1(T), \ldots, s_{36}(T)\} = \{x(T)_i x(T)_j : 1 \leq i \leq j \leq 8\}.$$

We also fix a representative

$$\sum_{j=1}^{8}\sum_{l=1}^{8}\lambda_{T,j,l}y_jy_l$$

of $\pi_T(\overline{R_1(B)})$, where

$$\lambda_{T,j,l}=\sum_{m=1}^{36}\mu_{T,j,l,m}s_m(T)$$

is linear in the $s_m(T)$ and we require that $\lambda_{T,1,8}=0$, which uniquely determines our representative.

From (4.8) we know that we must have

$$\lambda_{T,j,l}=0$$

for all j,l and for all $T\in J[2]$ and thus we get linear equations

$$\sum_{m}^{36}\mu_{T,j,l,m}s_m(T)=0$$

.

Let $S=(s_{ij})_{1\leq i\leq 36,1\leq j\leq 64}$ denote the matrix defined by $s_{ij}:=s_i(T_j)$, where $J[2]=\{T_1,\ldots,T_{64}\}$. It can be shown that this matrix has generic rank equal to 35, so any linear relation between the $s_i(T)$ satisfied by all $T\in J[2]$ must be a multiple of $R_1(x(T)_1,\ldots,x(T)_8)$. Hence $\overline{R_1(B)}$ must vanish.

The upshot of this is that if we require our $B_{ij}(x,y)$ to contain no multiples of, say, x_1x_8 or y_1y_8 as summands (which we can always arrange by applying (4.5)), then $R_1(B)=0$ follows. But this cannot hold in general: For example, take $P\in J\setminus J[2]$ and x a set of Kummer coordinates for P. We must have that $B_{ij}(x,x)$ lies in the ideal generated by the relations $R_1,\ldots,R_{35}$ for all $1\leq i,j\leq 7$, but $B_{18}(x,x)$ does not. This already implies that $R_1(B)$ cannot vanish in general and so not all of the B_{ij} can be correct. □

This result implies that the situation is much more complicated than in genus 2. We now analyze where this difficulty comes from.

Recall Flynn's strategy to compute the biquadratic forms in genus 2 (see [41] or [20]): If $T\in J[2]$, then we can compute

$$\kappa_i(P+T)\kappa_j(P-T)+\kappa_j(P+T)\kappa_i(P-T)=2\kappa_i(P+T)\kappa_j(P+T)$$

projectively for all i,j by multiplying the matrix W_T by the vector $\kappa(P)\in l^4$. Using some algebraic manipulations, Flynn ensures that the resulting B'_{ij}

are biquadratic in the $\kappa_i(P)$ and the $\kappa_j(T)$ and satisfy some additional normalization conditions. One can then check that the space of all $\kappa_i(T)\kappa_j(T)$, where $i \leq j$, is linearly independent of dimension 10. Hence for each pair (i, j) at most one biquadratic form that satisfies the same normalization conditions can specialize to B'_{ij}.

The crucial point is that from classical theory of theta functions we already know that such biquadratic forms B_{ij} must exist – at least in the complex case (see Hudson's book [54]) and thus, using the Lefshetz principle, for any algebraically closed field of characteristic 0. Therefore Flynn concludes that $B_{ij} = B'_{ij}$ for all i, j.

We can try to use the same strategy in the genus 3 case. Indeed, in [32], Duquesne computes the correct $B'_{ij}(x, y)$ in the special case that x is a set of Kummer coordinates for $T \in J[2]$. They can be downloaded from [35]. Because of the relation (4.5), we know that the space of all $\kappa_i(T)\kappa_j(T)$, where $i \leq j$, is not linearly independent. But we also know that it has dimension 35, that is R_1 is the only quadratic relation up to a constant factor. We have already used this fact in the proof of Proposition 4.5.

Now we can apply $R_1(x)$ and $R_1(y)$ to the $B'_{ij}(x, y)$ to make sure that no terms containing, say x_1x_8 or y_1y_8 appear and this is done by Duquesne. Thus we can draw the same conclusion as in the genus 2 situation, namely that for each pair (i, j) at most one biquadratic form that satisfies the same normalization conditions can specialize to B'_{ij}.

However, in the present situation it is not true that we know a priori that such biquadratic forms exist. Duquesne assumes this and claims that the B'_{ij} are the correct biquadratic forms for general x, y, but this must be false according to Proposition 4.5. The problem is that, in more modern language, the theta function formulas given by Hudson for Kummer surfaces are obtained by pushing points back and forth through $(2, 2)$-isogenies of abelian surfaces, see [45]. While every abelian surface over $\mathbb{C}$ is a hyperelliptic Jacobian surface, this is no longer the case for abelian threefolds, which suggests that it will at least be very difficult to generalize Hudson's formulas.

Yet at this point not all is lost: It could be the case that there are no biquadratic forms with the desired properties globally, but that we can find such forms locally, or it might still be possible to compute the B_{ij}, locally, or globally, even if they are of higher degree.

Let us first show that such forms must exist. We can embed $\mathrm{Sym}^2 K$ into $\mathbb{P}^{35}$ using the embedding

$$\iota : \{(x_1, \ldots, x_8), (y_1, \ldots, y_8)\} \mapsto (z_1, \ldots, z_{35}),$$

where

$$\begin{aligned} z_1 &= x_1y_1, \\ z_2 &= x_1y_2 + x_2y_1, \\ z_3 &= x_1y_3 + x_3y_1, \\ &\vdots \\ z_{36} &= x_8y_8. \end{aligned}$$

Consider the morphism

$$\begin{aligned} \phi_J : J \times J &\longrightarrow J \times J \\ (P, Q) &\mapsto (P + Q, P - Q). \end{aligned}$$

This morphism has degree $64 = 4^g$, since a pair $(P, Q) \in J \times J$ lies in the kernel of ϕ_J if and only if $P = Q \in J[2]$. We have

$$\#J[2] = \dim(\mathcal{L}(4\Theta)) = 4^g$$

by Riemann-Roch.

Now ϕ_J induces a morphism

$$\begin{aligned} \phi_K : \mathrm{Sym}^2 K &\longrightarrow \mathrm{Sym}^2 K \\ \{\kappa(P), \kappa(Q)\} &\mapsto \{\kappa(P + Q), \kappa(P - Q)\} \end{aligned}$$

and so there is another morphism $\psi : \mathbb{P}^{35} \longrightarrow \mathbb{P}^{35}$ such that the diagram

$$\begin{array}{ccc} J \times J & \xrightarrow{\phi_J} & J \times J \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ \mathrm{Sym}^2 K & \xrightarrow{\phi_K} & \mathrm{Sym}^2 K \\ \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\ \mathbb{P}^{35} & \xrightarrow{\psi} & \mathbb{P}^{35} \end{array}$$

is commutative. Hence there are, at least locally, forms

$$B_{ij}(x, y) : \mathrm{Sym}^2 K \longrightarrow \mathrm{Sym}^2 K$$

where

$$\begin{aligned} B_{11}(x, y) &= \psi_1(\iota(x, y)), \\ B_{12}(x, y) &= \psi_2(\iota(x, y)), \\ B_{13}(x, y) &= \psi_3(\iota(x, y)), \\ &\vdots \\ B_{88}(x, y) &= \psi_{36}(\iota(x, y)) \end{aligned}$$

such that if x and y are Kummer coordinates of $P, Q \in J$, respectively, then there are Kummer coordinates w and z for $P+Q$ and $P-Q$, respectively, satisfying

$$w * z = B(x, y),$$

where we set $B_{ij} = B_{ji}$ for $j < i$.

A natural approach to the problem of finding the B_{ij} is to use the geometric group law on J. If $P, Q \in J$ are generic, that is P is represented by

$$((x_1, y_1)) + ((x_2, y_2)) + ((x_3, y_3)) - 3(\infty),$$

where x_1, x_2 and x_3 are pairwise distinct, Q is represented by

$$((x_4, y_4)) + ((x_5, y_5)) + ((x_6, y_6)) - 3(\infty),$$

where x_4, x_5 and x_6 are pairwise distinct and $-(P+Q)$ is represented by

$$((x_7, y_7)) + ((x_8, y_8)) + ((x_9, y_9)) - 3(\infty),$$

where x_7, x_8 and x_9 are pairwise distinct, then there is a quartic $M(x)$ and a scalar γ such that the intersection of C with

$$(x - \gamma)y = M(x)$$

consists of the points (x_i, y_i) for $i = 1, \ldots, 9$. This was already used by Duquesne in [32] to find the matrix W_T representing translation by a 2-torsion point T.

It is quite easy to compute γ and $M(x)$ from $x_1, \ldots, x_6$ and $y_1, \ldots, y_6$. Thus we can express the points $(x_7, y_7), (x_8, y_8)$ and (x_9, y_9) – and of course also their images under the hyperelliptic involution – in terms of $x_1, \ldots, x_6$ and $y_1, \ldots, y_6$, which then gives us an expression of all

$$\kappa_i(P+Q)\kappa_j(P-Q) + \kappa_j(P+Q)\kappa_i(P-Q),\ i \neq j$$

and

$$\kappa_i(P+Q)\kappa_i(P-Q).$$

However, in general these expressions are too large to handle with current computing facilities. But one can consider specific curves C (or a family of curves depending on one parameter) and fix one of the points Q, say.

The next step is to write the results in terms of $\kappa_1(P), \ldots, \kappa_8(P)$ and $\kappa_1(Q), \ldots, \kappa_8(Q)$. We have attempted this in a joint effort with Sylvain Duquesne and it is possible in this way to recover the B'_{ij} for $1 \leq i, j \leq 4$, so in these examples we have that at least locally the desired forms B_{ij} are indeed biquadratic for all $1 \leq i, j \leq 4$, giving some partial justification for part (a) of Conjecture 4.7 below.

However, Duquesne has proved the following by explicit algebraic manipulation.

Example 4.6. (Duquesne) Let

$$F(X,1) = 4 + X^2 + X^3 + 4X^4 + 2X^5 - 4X^6 + X^7$$

and consider the points

$$Q = [((0,2)) + ((1,3)) + ((-1,1)) - 3(\infty)]$$

and

$$P = [((x_1,y_1)) + ((4,y_2)) + ((2,4)) - 3(\infty)],$$

where y_2 is determined up to sign and y_1 is determined up to sign by x_1 which is arbitrary. Then $\kappa_4(P)\kappa_5(Q) + \kappa_5(P)\kappa_4(Q)$ is not quadratic or quartic in $\kappa_1(P), \ldots, \kappa_8(P)$.

But it may still be possible to learn something from explicit examples. Let x and y denote Kummer coordinates for some fixed $P, Q \in J$, respectively. Because we can add points on the Jacobian easily in specific situations, we can compute the images of $P+Q$ and $P-Q$ on the Kummer threefold. As a next step, we analyze the biquadratic forms $B'_{ij}(x,y)$ computed by Duquesne.

We define two index sets

$$I := \{(i,j) : 1 \le i \le j \le 8\},$$

and

$$E := \{(1,8),(2,7),(3,6),(4,5),(5,5),(5,6),(5,7),(6,6)\}.$$

For now we assume that $B'_{i_0j_0}(x,y) \neq 0$ for some $(i_0,j_0) \in I \setminus E$. Let w and z denote Kummer coordinates for $P+Q$ and $P-Q$, respectively, normalized such that $w_{i_0}z_{j_0} = B'_{i_0j_0}(x,y)$.

We can check how far the $B'_{ij}(x,y)$ are away from the correct forms as follows. Let

$$\alpha_{ij}(x,y) := w_iz_j + w_jz_i - B'_{ij}(x,y) \quad \text{for } 1 \le i,j \le 8. \tag{4.9}$$

Building on a large number of numerical experiments we state a list of conjectures regarding the relations between $B'_{ij}(x,y)$ and $w_iz_j + w_jz_i$:

Conjecture 4.7. *The functions α_{ij} satisfy the following properties, where $x, y \in K_{\mathbb{A}}$:*

(a) We have $\alpha_{ij}(x,y) = 0$ for $(i,j) \in I \setminus E$.

(b) The identities

$$-\alpha_{1,8}(x,y) = \alpha_{2,7}(x,y) = \alpha_{3,6}(x,y) = \alpha_{4,5}(x,y)$$

and

$$\alpha_{5,7}(x,y) = -2\alpha_{6,6}(x,y)$$

hold.

(c) If $\alpha_{i_1 j_1}(x, y) = 0$ for some $(i_1, j_1) \in E$, then all $\alpha_{ij}(x, y)$ vanish.

(d) If $\alpha_{i_1 j_1}(x, y) \neq 0$ for some $(i_1, j_1) \in E$, then we have $\alpha_{ij}(x, y) \neq 0$ for all $(i, j) \in E$. If $(i, j), (i'j') \in E$, then the ratios

$$\frac{\alpha_{i'j'}(x, y)}{\alpha_{ij}(x, y)},$$

only depend on C and on $(i, j), (i', j')$, but not on x and y.

In large parts of Chapter 3 we were not required to work with the biquadratic forms B_{ij}, but rather with the quartic duplication polynomials δ which, however, were originally derived from the B_{ij}. If we assume the validity of the first two parts of Conjecture 4.7, then we can find analogs of these polynomials which again turn out to be quartic, although the B_{ij} are not all biquadratic.

More precisely, we temporarily assume that the characteristic of l is not equal to 3 and define

$$\delta_i(x) := B'_{i8}(x, x) \quad \text{for } i = 2, \ldots, 8,$$

and

$$\delta_1(x) := \frac{4}{3} B'_{18}(x, x).$$

Let $\delta(x) := (\delta_1(x), \ldots, \delta_8(x))$.

Conjecture 4.8. *Suppose that* $\mathrm{char}(l) \neq 3$. *Then we have*

$$\delta(\kappa(P)) = \kappa(2P)$$

for all $P \in J$.

We can relate this conjecture to our earlier Conjecture 4.7.

Lemma 4.9. *Suppose that parts (a) and (b) of Conjecture 4.7 are satisfied for C. Then Conjecture 4.8 follows.*

Proof. Let $P \in J$ and let x be a set of Kummer coordinates for P. Assuming part (a) of Conjecture 4.7, we can find a set $z \in K_{\mathbb{A}}$ of Kummer coordinates for $2P$ such that $z_i = \delta_i(x)$ for $i = 2, \ldots, 8$, because we have $\kappa(0) = (0, 0, 0, 0, 0, 0, 0, 1)$. Therefore it suffices to show that part (b) of Conjecture 4.7 implies that

$$z_1 = \frac{4}{3} B'_{18}(x, x). \tag{4.10}$$

Let $y \in K_{\mathbb{A}}$, fix Kummer coordinates z and w for $P + Q$ and $P - Q$, respectively, as above, and let α_{ij} be defined as in (4.9). For simplicity, let b_{ij} denote $w_i z_j + w_j z_i$ for $1 \leq i \neq j \leq 8$ and let b_{ii} denote $w_i z_i$ for $1 \leq i \leq 8$.

By construction, the B'_{ij} satisfy $R_1(B') = 0$ (see (4.7)) and so we have

$$B'_{18} - B'_{27} - B'_{36} - B'_{45} = 2f_5B'_{24} + 2f_5B'_{33} + 2f_6B'_{34} + 6f_7B'_{44}.$$

But applying the B'_{ij} to the pair (x, y) and using Conjecture 4.7 (b), we get that the left hand side is equal to

$$b_{18} - b_{27} - b_{36} - b_{45} - 4\alpha,$$

where $\alpha = \alpha_{1,8}(x, y)$, and that the right hand side is equal to

$$2f_5b_{24} + 2f_5b_{33} + 2f_6b_{34} + 6f_7b_{44}.$$

Setting $y = x$, we find that all b_{ij} must vanish unless $i = 8$ or $j = 8$ and so we obtain

$$b_{18} = 4\alpha.$$

Hence we conclude

$$z_1 = b_{18} = 4(b_{18} - B'_{18}(x, x)),$$

which proves (4.10) and thus the Lemma. □

Of course the δ_i are only well-defined up to the defining equations of K. But if Conjecture 4.8 holds, then at least the duplication law on the Kummer threefold can be expressed using quartic polynomials, in analogy with the situation in genus 2.

If we want to use the δ_i to define and compute canonical local heights, there is an additional problem; namely, in order to define local error functions ε_v as in (3.7) we need that

1) $\delta_i \in \mathbb{Z}[f_0, \ldots, f_7][x_1, \ldots, x_8]$ for all $i = 1, \ldots, 8$;

2) $\delta(0, 0, 0, 0, 0, 0, 0, 1) = (0, 0, 0, 0, 0, 0, 0, 1)$.

Neither of these is satisfied here. The only δ_i violating 1) is δ_1, some of whose coefficients have 3 as denominator. In order to repair this, we find a linear combination of quartic relations on K which added to $3\delta_1$ results in a quartic form whose coefficients are all divisible by 3. Dividing this polynomial by 3 and leaving the other δ_i unchanged, we get a tuple of homogeneous quartic polynomials satisfing 1). In particular we can drop the requirement that $\mathrm{char}(l) \neq 3$.

Concerning requirement 2), we have

$$\delta(0, 0, 0, 0, 0, 0, 0, 1) = (0, 0, 0, 0, 0, 0, 0, f_7^2).$$

But this can be repaired easily. Namely, we use the following transformation of models of K:

$$\begin{array}{rcl} \tau : K & \longrightarrow & K' \\ (x_1, \ldots, x_8) & \mapsto & (x_1, \ldots, x_7, f_7x_8) \end{array}$$

and let $\delta' : K' \longrightarrow K'$ be the map of degree 4 that makes the following diagram commute:

$$\begin{array}{ccc} K & \xrightarrow{\delta} & K \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau} \\ K' & \xrightarrow{\delta'} & K' \end{array} .$$

The map δ' is given explicitly by

$$\delta'(x_1, \ldots, x_8) = \left(\frac{\delta_1(x')}{f_7}, \ldots, \frac{\delta_7(x')}{f_7}, \delta_8(x') \right),$$

where $x' = (f_7 x_1, \ldots, f_7 x_7, x_8)$. Upon dividing all coefficients of the δ_i' by f_7^2 we find duplication polynomials on K' satisfying 2) under the assumption that Conjecture 4.8 is satisfied. Since most of what we do in the following relies on the validity of this conjecture, it is crucial for the future development of the present approach to prove it, for instance by proving parts (a) and (b) of Conjecture 4.7. In the next chapter we shall discuss a different approach which does not rely on any conjecture.

4.4 Canonical local heights on Jacobians

In this section we try to generalize our construction of canonical local heights from Section 3.4. The discussion is kept brief, because such results are not directly applicable in practice at the moment, since even in the hyperelliptic genus 3 case the results depend on the validity of Conjecture 4.8. Therefore we might as well work in a more general setting. Let C denote a smooth projective curve defined over the completion k_v of a number field or one-dimensional function field k at a place $v \in M_k$. Let J be the Jacobian of C and let K be its Kummer variety, embedded into projective space using a map

$$\kappa : J \longrightarrow K \hookrightarrow \mathbb{P}^{2^g - 1}$$

such that $\kappa(O) = (0, \ldots, 0, 1)$. Let $g_1, \ldots, g_N \in k_v$ denote the coefficients appearing in the given model of C. Suppose we have homogeneous quartic polynomials

$$\delta_i(x_1, \ldots, x_{2^g}) \in \mathbb{Z}[g_1, \ldots, g_N, x_1, \ldots, x_{2^g}]$$

such that

$$\delta := (\delta_1, \ldots, \delta_{2^g}) : K \longrightarrow K$$

makes the diagram

$$\begin{array}{ccc} J & \xrightarrow{[2]} & J \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ K & \xrightarrow{\delta} & K \end{array}$$

commute and such that

$$\delta(0,\dots,0,1) = (0,\dots,0,1).$$

Example 4.10. These conditions are, of course, satisfied in our constructions in Chapters 2 and 3. They are also satisfied in the situation of a hyperelliptic curve of genus 3 given by a model of the form (4.2) when $\mathrm{char}(k_v) \neq 2$, provided Conjecture 4.8 holds; namely, we can pick K' and δ' constructed at the end of the previous section as K and δ.

In this situation essentially all our definitions from Chapter 3 carry over. We define *Kummer coordinates on* K and the set $K_{\mathbb{A}}$ as in Definition 4.4.

Definition 4.11. Let $x \in K_{\mathbb{A}}(k_v)$ be a set of Kummer coordinates on K. Then we set

$$\varepsilon_v(x) := v(\delta(x)) - 4v(x)$$

and

$$\mu_v(x) = \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \varepsilon_v(\delta^{\circ n}(x)).$$

For the next definition recall the definitions of the local normalization constants N_v and n_v and of the global normalization constant d_k introduced in Section 1.1. Their purpose is to make the product formula (1.1) work for k.

Definition 4.12. Let $x \in K_{\mathbb{A}}(k_v)$ be a set of Kummer coordinates on K. The *naive local height of* x is the quantity

$$\lambda_v(x) := -\frac{N_v}{n_v} v(x)$$

and the *canonical local height of* x is given by

$$\hat{\lambda}_v(x) := -\frac{N_v}{n_v}(v(x) + \mu_v(x)).$$

It follows that if k is a number field or function field of dimension 1 and we assume that C is in fact defined over k, then we have

$$h(P) = \frac{1}{d_k} \sum_{v \in M_k} n_v \lambda_v(x)$$

and

$$\hat{h}(P) = \frac{1}{d_k} \sum_{v \in M_k} n_v \hat{\lambda}_v(x)$$

for any choice x of Kummer coordinates for $P \in J(k)$, where

$$h(P) = h(\kappa(P))$$

is the *naive height of* P and

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h\left(2^n P\right)$$

is the *canonical height of* P. If k is a global field, then we can in principle compute the canonical height using the algorithm due to Flynn and Smart as introduced in Section 3.2.2 if we can compute $\mu_v(P)$ for $v \in M_k^\infty$ and $P \in J(k)$. But the method outlined in that section requires a bound on the archimedean local height constant for each $v \in M_k^\infty$ and we have no such bounds available at the moment, even for our rather special hyperelliptic genus 3 curves. One possible method for the calculation of height constant bounds – the decomposition of the duplication map into Richelot isogenies as in [42] – is probably difficult to generalize and only leads to rather crude bounds even in genus 2. It seems more promising to use Stoll's representation-theoretic approach introduced in [92], but we have not attempted to do this.

Fortunately we can always compute archimedean canonical local heights using theta functions; we discuss this approach in 4.4.2.

One result from Chapter 3 which generalizes immediately is the following.

Proposition 4.13. *Let $\alpha : J \to J'$ be an isogeny of Jacobians defined over k_v and let $d = \deg(\alpha)$. Then α induces a map $\alpha : K \to K'$ between the corresponding Kummer varieties. We also get a well-defined induced map $\alpha : K_{\mathbb{A}} \longrightarrow K'_{\mathbb{A}}$ if we fix $a \in k_v^*$ and require $\alpha(0,0,0,1) = a(0,0,0,1)$. Moreover, we have*

$$\hat{\lambda}_v(\alpha(x)) = d\hat{\lambda}_v(x) + \log|a|_v$$

for any $x \in K_{\mathbb{A}}(k_v)$.

Proof. See the proof of Proposition 3.24. □

In particular we can control how the canonical local height changes when we change the model of C. For instance, suppose that C is hyperelliptic and

$$\tau = ([a,b,c,d], e, U)$$

is a change of model of C as in (3.16). Then τ induces a transformation τ on $K_{\mathbb{A}}$ that is a linear map on $\mathbb{A}^{2g}$. Let $v(\tau)$ denote the valuation of its determinant; then we get

$$\hat{\lambda}_v(\tau(x)) = \hat{\lambda}_v(x) - \frac{N_v}{n_v} v(\tau)$$

in analogy with Corollary 3.25.

4.4.1 Non-archimedean places

Suppose now that $v \in M_k$ is non-archimedean. A particularly useful observation in Chapter 3 was Theorem 3.29, stating that the set

$$U_v := \{P \in J(k_v) : \varepsilon_v(P) = 0\}$$

is a subgroup of $J(k_v)$ if $g = 2$. Unfortunately, it is not possible to imitate the proof given by Stoll in [94] in the higher genus situation, because we need to have the forms B_{ij} available explicitly. Once these are found, it should not be hard to prove an analog of Theorem 3.29 for hyperelliptic curves of genus 3 when $\mathrm{char}(k) \neq 2$.

In any event, the following conditional statement is immediate:

Theorem 4.14. *Suppose C is given by an $\mathcal{O}_v$-integral model whose closure $\mathcal{C}$ over $\mathrm{Spec}(\mathcal{O}_v)$ is normal and flat and has rational singularities. Suppose that the set U_v is a subgroup of $J(k_v)$. Then ε_v and μ_v factor through the component group Φ_v of the Néron model of J.*

Proof. This is the same as the proof of Theorem 3.30, since we can define canonical local heights with respect to certain divisors D_i, where $i \in \{1, \ldots, 2^g\}$ as in the previous chapter. □

The previous result may also be useful for theoretical investigations. For practical purposes, we first have to find the forms B_{ij} or at least prove Conjecture 4.7, parts (a) and (b). In principle it should also be possible to generalize the simplification procedure introduced in Section 3.4.4 and then find formulas for a small number of models that we can always, using Proposition 4.13, reduce to; yet the difficulties we have encountered handling the much easier genus 2 situation suggest that this should be a very tedious task.

4.4.2 Archimedean places

In order to compute archimedean canonical local height we introduced several methods in the previous chapters, one of which turns out to generalize immediately. Let $v \in M_k$ be archimedean and consider $C(\mathbb{C})$ as a Riemann surface embedded into complex projective space using v.

Because we can change the model, we suppose that the embedding κ corresponds to $\mathcal{L}(2\Theta)$, where Θ is the theta divisor corresponding to the Abel-Jacobi map embedding C into J using some fixed base point. Let $\tau_v \in \mathfrak{h}_g$ such that $J(\mathbb{C})$ is isomorphic to $\mathbb{C}^g/\Lambda_v$, where $\Lambda_v = \mathbb{Z}^g \oplus \tau_v\mathbb{Z}^g$ and define j by

$$j : \mathbb{C}^g \longrightarrow\!\!\!\!\!\rightarrow \mathbb{C}^g/\Lambda_v \xrightarrow{\cong} J(\mathbb{C}).$$

Let $a = (1/2, \ldots, 1/2), b = (g/2, (g-1)/2 \ldots, 1, 1/2) \in \mathbb{C}^g$ and let $\theta_{a,b}$ denote the theta function with characteristic $[a; b]$ defined in Section 1.6.

Proposition 4.15. *(Pazuki) The function $\theta_{a,b}$ has divisor $j^*(\Theta)$. Moreover, the following function is a Néron function associated with Θ and v:*

$$\hat{\lambda}'_{\Theta,v}(P) = -\log|\theta_{a,b}(z(P))|_v + \pi \operatorname{Im}(z(P))^T (\operatorname{Im}(\tau_v))^{-1} \operatorname{Im}(z(P)),$$

where $j(z(P)) = P$.

Proof. See the proof of Proposition 3.77. □

Hence we can use $\hat{\lambda}'_{\Theta,v}$ to compute λ_v, because as in Section 3.7.2, there must be a constant d_v such that

$$\hat{\lambda}_v(P) = 2\hat{\lambda}'_{\Theta,v}(P) + d_v$$

for all $P \in J(\mathbb{C}) \setminus \operatorname{supp}(\Theta)$, where

$$\hat{\lambda}_v(P) = \hat{\lambda}_v(\kappa(P)/\kappa_1(P)).$$

We can find the constant d_v using a 3-torsion point as in (3.31) and compute $\lambda_v(P)$ for all $P \in J(\mathbb{C}) \setminus \operatorname{supp}(\Theta)$; other points can be treated similarly. For this we can use the existing implementation of theta functions in `Magma` mentioned in Section 3.7.2.

Chapter 5

Arithmetic intersection theory

We have seen in the previous chapter that the computation of canonical heights using the decomposition into canonical local heights becomes quite complicated as we increase the genus. It proved to be rather successful in Chapters 2 and 3, but it runs into problems even in the case of Jacobians of hyperelliptic curves of genus 3 with a rational Weierstrass point. Since the main problems lie in the complexity of the associated Kummer variety and how the group law on the Jacobian is reflected on it, it is not very likely that this situation will improve for other curves of genus at least 3.

In the present chapter we use a different approach to develop a practical algorithm for the computation of canonical heights on Jacobians. However, in contrast to the previous chapters, it does not come with a naive height combining the properties that we can list all points of naive height up to some bound and that the difference between the two heights can be bounded effectively. In the hyperelliptic genus 3 case, it might be possible to combine the method that we are about to discuss with the Kummer threefold approach.

5.1 Local Néron symbols

In this section we discuss the theory of local Néron symbols whose existence was first proved by Néron in [78]. We shall present an interpretation that is suitable for explicit computations, following essentially Gross [46] and Hriljac [53]. The content of the latter work is also discussed by Lang in [60]. In order to present these results, we need the definitions and results of Section 1.5, especially the intersection theory on arithmetic surfaces.

Let R be a discrete valuation ring with valuation v, let l be the field of fractions of R and let $S = \mathrm{Spec}(R)$. Let C be a smooth projective geometrically connected curve of positive genus g defined over l and let $\chi : \mathcal{C} \to S$ denote a C over S.

Consider divisors on $C \cong \mathcal{C}_l$. Recall that we denote the group of l-rational divisors on C by $\mathrm{Div}(C)(l)$. For each $n \in \mathbb{Z}$ the group $\mathrm{Div}^n(C)$ is defined to be the group of divisors of degree equal to n and we set

$$\mathrm{Div}^n(C)(l) := \mathrm{Div}^n(C) \cap \mathrm{Div}(C)(l).$$

We are particularly interested in the case $n = 0$.

If $D \in \mathrm{Div}(C)(l)$ is prime, then we write $D_{\mathcal{C}}$ for the closure of D on $\mathcal{C}$ as in Section 1.4. This is a prime horizontal divisor on $\mathcal{C}$ and we extend the operation $D \mapsto D_{\mathcal{C}}$ to $\mathrm{Div}(C)(l)$ by linearity.

For the remainder of this section, we fix a regular model $\mathcal{C}'$ of C over S. In order to define local Néron symbols we need to deal with fibral $\mathbb{Q}$-divisors. Let $\mathbb{Q}\,\mathrm{Div}_v(\mathcal{C}')$ denote the $\mathbb{Q}$-vector spaces generated by the irreducible com-

ponents of $\mathcal{C}'_v$ and let $\mathbb{Q}\mathcal{C}'_v$ denote the $\mathbb{Q}$-vector space generated by the whole fiber $\mathcal{C}'_v$.

Lemma 5.1. *There exists a unique linear map*

$$\Phi_{v,\mathcal{C}'} : \mathrm{Div}^0(C)(l) \to \mathbb{Q}\,\mathrm{Div}_v(\mathcal{C}')/\mathbb{Q}\mathcal{C}'_v,$$

such that for all $D \in \mathrm{Div}^0(C)(l)$ the $\mathbb{Q}$-divisor $D_{\mathcal{C}'} + \Phi_{v,\mathcal{C}'}(D)$ is orthogonal to $\mathrm{Div}_v(\mathcal{C}')$ with respect to $i_v(\cdot,\cdot)$.

Proof. Let $\mathcal{C}'_v = \sum_{i=0}^r n_i \Gamma_v^i$ be the decomposition of $\mathcal{C}'_v$ as a divisor, where $\Gamma_v^0, \ldots, \Gamma_v^r$ are the irreducible components of $\mathcal{C}'_v$. Let M_v be the intersection matrix $\left(i_v(n_i\Gamma_v^i, n_j\Gamma_v^j)\right)_{0\le i,j\le r}$ of $\mathcal{C}'_v$ and let

$$M : \mathbb{Q}\,\mathrm{Div}_v(\mathcal{C}') \longrightarrow \mathbb{Q}^{r+1}$$

be the linear map defined by

$$E \mapsto \left(n_0 i_v(E,\Gamma_v^0), \ldots, n_r i_v(E,\Gamma_v^r)\right)^T.$$

Lemma 1.30 implies that the kernel of M is $\mathbb{Q}\mathcal{C}'_v$, hence we get an induced map $\widetilde{M} : \mathbb{Q}\,\mathrm{Div}_v(\mathcal{C}'))/\mathbb{Q}\mathcal{C}'_v \longrightarrow \mathbb{Q}^{r+1}$ and there is a unique solution of

$$\widetilde{M}(\Phi_{v,\mathcal{C}'}(D)) = -s(D),$$

where $s(D) = \left(n_0 i_v(D_{\mathcal{C}'}, \Gamma_v^0), \ldots, n_r i_v(D_{\mathcal{C}'}, \Gamma_v^r)\right)^T$. □

By abuse of notation we denote a representative of $\Phi_{v,\mathcal{C}'}(D)$ also by $\Phi_{v,\mathcal{C}'}(D)$, since in our intended application it does not matter which representative we choose. Now we have assembled all ingredients necessary to define the central objects of this chapter in the non-archimedean case.

Definition 5.2. The *local Néron symbol on C over l* is the pairing

$$\langle D, E\rangle_v := i_v(D_{\mathcal{C}'} + \Phi_{v,\mathcal{C}'}(D), E_{\mathcal{C}'}) \log q_v,$$

defined on divisors $D, E \in \mathrm{Div}^0(C)(l)$ with disjoint support.

Remark 5.3. The proper regular model $\mathcal{C}'$ that is crucial for the construction of the local Néron symbol does not show up in this notation. This is justified by part (e) of Proposition 5.7 below. Also note that from the definitions and Lemma 1.30 we immediately get

$$\begin{aligned} i_v(D_{\mathcal{C}'} + \Phi_{v,\mathcal{C}'}(D), E_{\mathcal{C}'}) &= i_v(D_{\mathcal{C}'} + \Phi_{v,\mathcal{C}'}(D), E_{\mathcal{C}'} + \Phi_{v,\mathcal{C}'}(E)) \\ &= i_v(D_{\mathcal{C}'}, E_{\mathcal{C}'} + \Phi_{v,\mathcal{C}'}(E)). \end{aligned}$$

Next we consider an archimedean local field l and we want to define local Néron symbols over l. We can assume $l = \mathbb{C}$ (see part (g) of Proposition 5.7 below), so that $C(l)$ is actually a compact Riemann surface. For the construction of local Néron symbols we need the notion of *Green's functions* on Riemann surfaces.

Proposition 5.4. *Let X be a compact Riemann surface and let $d\mu$ be a positive volume form on X, normalized such that $\int_X d\mu = 1$. For each $D \in \mathrm{Div}(X)$ there exists a unique function*

$$g_D : X \setminus \mathrm{supp}(D) \to \mathbb{R},$$

called the Green's function with respect to D and $d\mu$, *such that the following properties are satisfied:*

(i) The function g_D is C^∞ outside of $\mathrm{supp}(D)$ *and has a logarithmic singularity along D, that is, if D is represented by a function f on an open subset U of X, then there is some $\alpha \in C^\infty(U)$ such that*

$$g_D(P) = -\log|f(P)| + \alpha(P)$$

holds for all $P \in U \setminus \mathrm{supp}(D)$.

(ii)

$$\deg(D)d\mu = \frac{i}{\pi}\partial\overline{\partial}g_D$$

(iii)

$$\int_X g_D d\mu = 0$$

Proof. See [60] for a proof of existence due to Coleman that uses differentials of third kind. In Section 5.3.6 we use a proof due to Hriljac (see [52]) and reproduced in [59] for the case where $d\mu$ is the canonical volume form on X, because it is rather constructive, at least for non-special divisors. For uniqueness, note that g_D is determined uniquely up to an additive constant by (i) and (ii), because the difference of two functions satisfying (i) and (ii) is harmonic everywhere and hence constant. Property (iii) fixes the constant. □

Remark 5.5. We call a function satisfying (i) and (ii) an *almost-Green's function with respect to D and $d\mu$.*

Let v be the absolute value on l, normalized as in Section 1.1 and fix a volume form $d\mu_v$ on $C(l)$, normalized as in the theorem above. For two divisors $D, E \in \mathrm{Div}(C)(l)$ with disjoint support we define the *intersection multiplicity of D and E* by

$$i_v(D, E) := g_D(E) := \sum_j m_j g_D(Q_j),$$

where $E = \sum_j m_j(Q_j)$.

Definition 5.6. We call the pairing $\langle \cdot, \cdot \rangle_v$ that associates to all $D, E \in \mathrm{Div}^0(C)(l)$ with disjoint support the number $i_v(D, E)$ the *local Néron symbol on C over l*.

Notice that in order to compute $\langle D, E \rangle_v$ for given $D, E \in \mathrm{Div}^0(C)(l)$ with disjoint support, we only need to find an almost-Green's function with respect to D and that property (ii) reduces to the requirement that g_D is harmonic. In particular, this restriction eliminates the dependency of the intersection multiplicity on the choice of $d\mu_v$.

We list the most important properties of the local Néron symbol, both archimedean and non-archimedean, in the following proposition. But first we need to introduce further notation. If $f \in l(C)^*$ and $E = \sum_j m_j(Q_j) \in \mathrm{Div}^0(C)(l)$, then we set

$$f(E) := \prod_j f(Q_j)^{m_j}.$$

Proposition 5.7. *(Néron, Gross, Hriljac) Let l be a field that is complete with respect to an absolute value v. The local Néron symbol satisfies the following properties, where $D, E \in \mathrm{Div}^0(C)(l)$ have disjoint support.*

(a) The symbol is bilinear.

(b) The symbol is symmetric.

(c) If $f \in l(C)^*$, then we have $\langle D, \mathrm{div}(f) \rangle_v = v(f(D))$.

(d) Fix $D \in \mathrm{Div}^0(l)$ and $P_0 \in C(l) \setminus \mathrm{supp}(D)$. Then the map $C(l) \setminus \mathrm{supp}(D) \longrightarrow \mathbb{R}$ defined by

$$P \mapsto \langle D, (P) - (P_0) \rangle_v$$

is continuous and locally bounded with respect to the v-adic topology.

(e) If v is non-archimedean, then $\langle D, E \rangle_v$ is independent of the choice of the proper regular model $\mathcal{C}'$ and of the choice of $\Phi_{v,\mathcal{C}'}(D)$.

(f) If v is archimedean, then $\langle D, E \rangle_v$ is independent of the choice of the volume form $d\mu_v$.

(g) If l' is an extension of l with valuation v' extending v, then we have $\langle D, E \rangle_v = \langle D, E \rangle_{v'}$.

Moreover, the pairing is uniquely determined by properties (a)–(d).

Proof. Existence and uniqueness of a pairing satisfying (a)–(d) was shown by Néron in [78] when $C(l)$ is Zariski dense in C. The construction of the pairing using arithmetic intersection theory that is presented in this section and the

proof that the pairing thus constructed coincides with Néron's abstractly defined pairing is due to Gross [46] and Hriljac [53].

When $C(l)$ is not Zariski dense in C, then Néron's proof does not apply. In this more general situation Néron shows that any pairing satisfying (a)–(c) and another condition (d') similar to (d) must be the local Néron symbol. Finally, Hriljac proves that the pairing constructed above satisfies (a)–(c) and (d'). We get (e), (f) and (g) for free because of the uniqueness property. □

Remark 5.8. One can define local Néron symbols for divisors with common support at the loss of some functoriality, see [46, §5].

5.2 Global Néron symbols and canonical heights

Recall our notation from Section 1.1: Let k denote a number field or a one-dimensional function field with ring of integers $\mathcal{O}_k$. Let C be a smooth projective geometrically connected curve of genus $g \geq 1$ defined over k. We assume that it is given by an $\mathcal{O}_k$-integral model.

If $D \in \mathrm{Div}(C)(k)$ and $v \in M_k$, then we denote by D_v the localization $D \otimes_k k_v$ of D at v. If $D, E \in \mathrm{Div}^0(C)(k)$, then we can add up all the local Néron symbols defined in the previous section, because only finitely many of them are nonzero. To see this, note that over all places of good reduction the closure $\mathcal{C}$ of the given model of C over $\mathrm{Spec}(\mathcal{O}_v)$ is a proper regular model over $\mathrm{Spec}(\mathcal{O}_v)$; using these closures for our computations we have $\Phi_{v,\mathcal{C}}(D_v) = 0$ for all such v and $i_v(D_{v,\mathcal{C}}, E_{v,\mathcal{C}}) \neq 0$ for only finitely many such v.

Definition 5.9. If $D, E \in \mathrm{Div}^0(C)(k)$ have disjoint support and $v \in M_k$, then we define

$$\langle D, E \rangle_v := \langle D_v, E_v \rangle_v.$$

We call the pairing associating to D, E the sum

$$\langle D, E \rangle := \sum_{v \in M_k} N_v \langle D, E \rangle_v$$

the *global Néron symbol*.

From parts (a) and (b) of Proposition 5.7 we get that this pairing is bilinear and symmetric. Because of (c) and the product formula it is also invariant under linear equivalence, so the global Néron symbol is actually defined on pairs of elements of $\mathrm{Pic}^0(C)(k)$ that are represented by k-rational divisors. Hence we can drop the assumption that D and E have disjoint support.

Theorem 5.11 below connects Néron symbols with canonical heights. In order to state it, we need to fix an ample symmetric k-rational divisor class on the Jacobian J of C, as the canonical height with respect to a divisor only depends on the linear equivalence class of the divisor.

Let K denote the Kummer variety $J/\{\pm 1\}$ of J. In analogy with our previous constructions we want to find a divisor T such that a basis of $\mathcal{L}(T)$ gives an embedding of K into $\mathbb{P}^{2^g-1}$. This can be accomplished as follows, see [46, §4]: Let W denote the image of $\mathrm{Sym}^{g-1}(C)$ in $\mathrm{Pic}^{g-1}(C)$ and let $c \in \mathrm{Pic}^{g-1}(C)$ be a divisor class such that $2c$ is equal to the canonical class of C. Then $W - c$ is a theta-divisor and the class of

$$T := 2(W - c) \in \mathrm{Div}(J)$$

is symmetric, ample and k-rational and hence satisfies all conditions that we need in order to define a canonical height. Furthermore it is independent of c and a basis of $\mathcal{L}(T)$ can be used to embed K into $\mathbb{P}^{2^g-1}$ as in Chapters 3 and 4.

Note that if C is an elliptic curve, then the linear equivalence class of T is equal to the class of $2(O)$, where O is the origin of C. More generally, if C is a hyperelliptic curve given as the smooth projective model of a hyperelliptic equation

$$Y^2 + H(X,1)Y = F(X,1)$$

with nonzero discriminant, then we have $[T] = 2[\Theta]$ if C has a k-rational Weierstrass point and Θ is the theta-divisor with respect to that point. If no such point exists, then $[T] = [\Theta^+ + \Theta^-]$ as in Section 3.1.

Recall the Definitions 1.2 and 1.42 of the canonical height and the associated height pairing.

Definition 5.10. Let C, J and T be as above. The *canonical height (or Néron-Tate height) on* J is the function

$$\hat{h}(\cdot) := \hat{h}_T(\cdot)$$

and the *canonical height pairing (or Néron-Tate height pairing) on* J is defined by

$$(\cdot,\cdot) := (\cdot,\cdot)_T.$$

Theorem 5.11. *(Faltings, Hriljac, Néron) Suppose C is a smooth projective geometrically connected curve of positive genus g defined over a number field or one-dimensional function field k. Suppose that $D, E \in \mathrm{Div}^0(C)(k)$ and denote their images on J by $J(D)$ and $J(E)$, respectively. Then we have*

$$\langle D, E\rangle = -(J(D), J(E))$$

and in particular

$$\langle D, D\rangle = -\hat{h}(J(D)).$$

Proof. Néron [78] first proved the theorem using existence and uniqueness of abstractly defined local Néron symbols (see Proposition 5.7). The proofs of Faltings [37] and Hriljac [52] use the interpretation of the local Néron symbol in terms of arithmetic intersection theory presented in Section 5.1. All of these proofs are stated for the number field case, but continue to hold in the case of one-dimensional function fields. In the latter situation, the first proof of the case $g = 1$ is due to Manin (cf. [89, Chapter III]). □

The practical importance of this result lies in the fact that we can, at least in principle, compute the canonical height on the Jacobian using data associated to the curve. We do not impose any further conditions on C (yet). Suppose that we are given a point $P \in J(k)$ and we want to compute its canonical height $\hat{h}(P)$. In order to use Theorem 5.11 for this purpose, we proceed as follows:

(1) Find divisors $D, E \in \mathrm{Div}^0(C)(k)$ such that $J(D) = J(E) = P$ and $\mathrm{supp}(D) \cap \mathrm{supp}(E) = \emptyset$.

(2) Determine the set U of places $v \in M_k^0$ such that $\langle D, E \rangle_v \neq 0$ is possible.

(3) Find a proper regular model $\mathcal{C}'$ of C over $\mathrm{Spec}(\mathcal{O}_v)$ for all $v \in U$ of bad reduction.

(4) Compute $i_v(D_{v,\mathcal{C}'}, E_{v,\mathcal{C}'})$ for all $v \in U$.

(5) Compute a representative of $\Phi_{v,\mathcal{C}'}(D_v)$ and $i_v(\Phi_{v,\mathcal{C}'}(D_{v,\mathcal{C}'}), E_{v,\mathcal{C}'})$ for all $v \in U$ of bad reduction.

(6) Find an almost-Green's function g_{D_v} and compute $g_{D_v}(E_v)$ for all $v \in M_k^\infty$.

(7) Sum up all local Néron symbols.

We deal with these steps in the following sections. After a few remarks we must, however, first discuss how divisors can be represented in practice.

Remark 5.12. We shall tacitly assume from now on that step (1) is always possible in principle, that is every P we encounter can be represented using a k-rational divisor. If, for instance, k is a global field, then [82, Proposition 3.3] implies that this is guaranteed whenever the curve has a k_v-rational divisor of degree 1 for all $v \in M_k$. If we are not in this situation, that is we have $P \in J(k)$ which cannot be represented using a k-rational divisor, then we have two options:

- Work over a field extension k'/k such that there exists some $D \in \mathrm{Div}^0(C)(k')$ satisfying $[D] = P$.
- Compute a multiple nP such that there exists $D \in \mathrm{Div}^0(C)(k)$ satisfying $[D] = nP$ and use the quadraticity of the canonical height.

The existence of n as in the latter approach follows from [82, Proposition 3.2]; we can take for n the period of C over k, that is the greatest common divisor of the degrees of all k-rational divisor classes.

Remark 5.13. We have only defined the global Néron symbol in terms of intersection multiplicities on $\mathrm{Div}^0(C)(k) \times \mathrm{Div}^0(C)(k)$, since that is all we need. However, the concepts introduced so far are in fact sufficient to define the notion of Arakelov intersection multiplicities for $D, E \in \mathrm{Div}(C)(k)$ with disjoint support as

$$(D, E)_{\mathrm{Ar}} := \sum_{v \in M_k^0} i_v(D_{v,\mathcal{C}'}, E_{v,\mathcal{C}'}) \log q_v + \sum_{v \in M_k^\infty} i_v(D_v, E_v) \tag{5.1}$$

after fixing a volume form $d\mu_v$ for each $v \in M_k^\infty$. However, this intersection pairing does not respect linear equivalence. In order to remedy this it can be extended to a generalized divisor group on a regular model of C over $\mathrm{Spec}(\mathcal{O}_k)$, called the Arakelov divisor group, such that it is invariant under (a suitably modified definition of) linear equivalence. See any expository work on Arakelov theory, such as [60] or [53]. The results of this chapter can also be viewed as a contribution to the problem of explicit computations of Arakelov intersection multiplicities.

Remark 5.14. For some of our intended applications we need more than merely the computation of the canonical height: According to Section 1.7 we also need to be able to list points up to bounded canonical height $\hat{h}(P)$. One way of doing this which has proved to be quite successful in genus 1 and 2 is to bound the difference between $\hat{h}(P)$ and $h(P)$ for $P \in J(k)$ and list points of bounded naive height $h(P)$. However, we are now faced with a new problem: In the previous chapters it was perfectly clear how to define a naive height such that both are possible (if not necessarily easy).

In the present situation we cannot work with an explicit embedding of the Kummer variety any longer and hence we need some new ideas. It would be desirable to develop a different method for listing points up to bounded canonical height which bypasses the need to use the naive height, but nobody seems to have an idea how to do this at the moment. If we want to use a naive height, then it is clear that this naive height should be given by a sum of local terms, one for each place of k, related to arithmetic intersection theory, so that bounding the difference becomes possible. Moreover, it is obviously a good idea to work on (regular models of the) curve as much as possible. See [51] for the recent construction of a promising naive height.

5.2.1 Representing and reducing divisors

The basic reference for large parts of the remainder of this section is [48]. If an ideal I is generated by $b_1, \ldots, b_n$, then we write $I = (b_1, \ldots, b_n)$. Let

l be an arbitrary field and let C denote a smooth projective geometrically connected curve of genus $g \geq 1$ defined over l. There are essentially two ways of representing a divisor $D \in \mathrm{Div}(C)(l)$.

(a) As a sum

$$D = \sum_i m_i D_i,$$

where $D_i \in \mathrm{Div}(C)(l)$ is irreducible over l and $m_i \in \mathbb{Z}$ for all i. We call this the *free representation of* D.

(b) Assuming D is effective, using a defining ideal

$$I_D \subset l[C].$$

We call this the *ideal representation of* D.

It often helps to view prime divisors over l as places of the function field $l(C)$. Most computations are done by first writing a general divisor as a difference of effective divisors and using their respective ideal representations.

Since in our intended applications we are allowed (and occasionally even required) to vary divisors in their linear equivalence classes, it is a natural question to ask whether it is possible to find divisors linearly equivalent to a given divisor in a way that facilitates explicit computations.

Lemma 5.15. *(Hess) For all $D \in \mathrm{Div}(C)(l)$ and effective $A \in \mathrm{Div}(C)(l)$ there exists an effectively computable triple $(\tilde{D}, r, a)$, where $\tilde{D} \in \mathrm{Div}(C)(l)$ is effective, $r \in \mathbb{Z}$ and $a \in l(C)$ such that $\deg(\tilde{D}) < g + \deg(A)$ and we have*

$$D = \tilde{D} + rA + \mathrm{div}(a).$$

We call $\tilde{D}$ a reduction *of D along A. If $\deg(A) = 1$, then $\tilde{D}$ is the unique effective divisor such that $\dim(\mathcal{L}(\tilde{D} - r'A)) = 0$ for all $r' \geq 1$. In this case we have $D \sim \tilde{D} + rA$, where $r \in \mathbb{Z}$ is the maximal integer such that $\dim(\mathcal{L}(D - rA)) = 1$.*

Proof. See [48, §8]. □

It is not obvious how to pick the effective, l-rational divisor A. If we have an l-rational divisor of degree 1 on C then this can be used. If C is a plane curve, then we can use the zero or pole divisor of a line, for instance the pole divisor $(x)_\infty$. In some situations we might want to pick distinct A, A' in order to reduce two divisors D, D' and at the same time separate their supports. But in general the choice of A (and possibly of A') depends on the specific situation.

5.2.2 Mumford representation of divisors on hyperelliptic curves

Suppose that C is a hyperelliptic curve of genus g defined over l, given as the smooth projective model of an equation

$$Y^2 + H(X,1)Y = F(X,1), \tag{5.2}$$

where $F(X,Z), H(X,Z) \in l[X,Z]$ are forms of degrees $2g+2$ and $g+1$, respectively, and the discriminant of the equation (5.2) is nonzero. Suppose that $D \in \mathrm{Div}(C)(l)$ has degree zero. Then the notions introduced in the previous section are all well-known: The reduction process is part of Cantor's algorithm for the addition of divisor classes introduced in [19]; here the divisor A used for reduction is equal to (∞) when we have an l-rational Weierstrass point ∞ at infinity and is equal to $(\infty^+)+(\infty^-)$ when there are two branches ∞^+, ∞^- over the singular point at infinity in the projective closure of equation (5.2) as in Chapter 3.

In the former case Lemma 5.15 says that the reduction process yields the unique effective $\tilde{D}$ such that

$$D \sim \tilde{D} + r(\infty),$$

where $0 \leq -r = \deg \tilde{D} \leq g$ and $\deg(\tilde{D})$ is minimal. In the latter case it turns out that when g is even we can still find a unique $\tilde{D}$ of minimal nonnegative even degree $-r \leq g$ such that

$$D \sim \tilde{D} + \frac{r}{2}((\infty^+) + (\infty^-))$$

if we impose further conditions on its ideal representation. Conversely, if g is odd we might have to take reductions of degree $g+1$ into account and these are not be unique. However, uniqueness of the reduction is not an essential property in our applications and so we shall not discuss it any further. The case $g = 3$ is discussed in Section 4.1.

The ideal representation of a reduced effective divisor D is given by the *Mumford representation* which we recall briefly below. Note that this has already been used in the proof of Proposition 3.12.

If we view C as embedded in weighted projective space of weights $1, g+1, 1$ assigned to the variables X, Y, Z, then it is given by the equation

$$Y^2 + H(X,Z)Y = F(X,Z).$$

An effective divisor D of degree $d \leq g+1$ corresponds to a pair of homogeneous forms $(A(X,Z), B(X,Z))$, where $A(X,Z)$ and $B(X,Z)$ have degrees d and $g+1$ respectively, such that D is defined by

$$A(X,Z) = 0 = Y - B(X,Z)$$

and we impose the additional condition that $A(X,Z)$ divides $B(X,Z)^2 + H(X,Z)B(X,Z) - F(X,Z)$.

First suppose that there is a unique Weierstrass point ∞ at infinity in $C(l)$. Then any nonzero effective divisor $D = \sum_{j=1}^{d}(P_j)$ that is reduced along (∞) has degree $d \leq g$ and cannot contain ∞ in its support. Hence we can safely dehomogenize in order to represent D and so we may take

$$I_D = (a(x), y - b(x)),$$

where $a(x) = A(x,1)$ and $b(x) = B(x,1)$, for its ideal representation. More concretely, we have

$$a(x) = \prod_{j=1}^{n}(x - x(P_j))$$

and $b(x)$ has minimal degree such that

$$b(x(P_j)) = y(P_j) \text{ for } j = 1, \ldots, d.$$

Conversely, suppose that there are two points ∞^+, ∞^- at infinity. Suppose that D is reduced along $(\infty^+) + (\infty^-)$. If $\mathrm{supp}(D)$ does not contain a point at infinity, then we can dehomogenize as before to find an affine representation. If this does not hold, say $\infty^+ \in \mathrm{supp}(D)$, then necessarily $\infty^+, \infty^- \in C(l)$ and $\infty^- \notin \mathrm{supp}(D)$. This case is more subtle, because we cannot tell the multiplicity of ∞^+ in D from its dehomogenized form. For our applications it suffices to treat the affine and the infinite part of D separately. Hence this complication does not cause any trouble.

5.3 Computing canonical heights using the global Néron symbol

In this section we shall address the steps needed for the computation of global Néron symbols introduced in the previous section. The first two steps are global in nature and can be viewed as preparatory steps for the remaining four sections which are local. We usually start with a general discussion and then specialize to certain situations where more precise statements or improvements are possible.

The case of hyperelliptic curves of odd degree has also been treated independently by Holmes, see [50], where some of the results of this section also appear; we shall point out when this is the case and also mention differences. We assume that C is a smooth projective geometrically connected curve over a number field or one-dimensional function field k given by an $\mathcal{O}_k$-integral model. Let J denote the Jacobian of C.

5.3.1 Finding suitable divisors of degree zero

Assume that we are given some divisor $D \in \mathrm{Div}^0(C)(k)$ such that $J(D) = P \in J(k)$ and we want to find $E \sim D$ such that E and D have disjoint support, that is, we are looking for an effective version of the moving lemma. However, we would like to keep the computations as simple as possible and this means that we would like to work with divisors that are reduced along some effective divisor of small degree whenever possible. This leads to the following method:

1. Pick two effective divisors $A, A' \in \mathrm{Div}(C)(k)$ with disjoint support.

2. Compute multiples nD, where $n = 1, -1, 2, -2, \ldots$ and reduce them along A and A' until we find some n and n' such that the reduction $\tilde{D}_n$ of nD along A and the reduction $\tilde{D}_{n'}$ of $n'D$ along A' have disjoint support.

3. Let $r_n, r_{n'} \in \mathbb{Z}$ such that $nD \sim \tilde{D}_n + r_n A$ and $n'D \sim \tilde{D'}_{n'} + r_{n'} A'$. Compute

$$\begin{aligned}\langle D, D\rangle &= \frac{1}{nn'}\langle \tilde{D}_n + r_n A, \tilde{D'}_{n'} + r_{n'} A'\rangle \\ &= \frac{1}{nn'}\langle \tilde{D}_n, \tilde{D'}_{n'}\rangle + \frac{r_n}{nn'}\langle A, \tilde{D'}_{n'}\rangle + \frac{r_{n'}}{nn'}\langle \tilde{D}_n, A'\rangle + \frac{r_n r_{n'}}{nn'}\langle A, A'\rangle.\end{aligned}$$

In practice integers n, n' of fairly small absolute value usually suffice.

For instance, let C be a hyperelliptic curves given by a model of the form (5.2). Let the divisor D_∞ be defined by $2(\infty)$ if there is a unique l-rational point at infinity and by $(\infty^+) + (\infty^-)$ otherwise. Also suppose d is even and

$$D = \tilde{D} - \frac{d}{2} D_\infty,$$

where $\tilde{D} = \sum_{i=1}^{d} (P_i)$ is reduced along D_∞, such that no P_i is a point at infinity or a Weierstrass point. Then we can always use $n_1 = 1$ and $n_2 = -1$ in the method introduced above; this is due to Holmes, see [50]. Namely, if we apply the hyperelliptic involution

$$Q \mapsto Q^-$$

to the points P_i, then we have

$$D' = \sum_{i=1}^{d} (P_i^-) - \frac{d}{2} D_\infty \sim -D.$$

If we move this by the divisor of a function $x - \zeta$, where $\zeta \in k$ is such that $x(P_i) \neq \zeta$ for all P_i, then we find

$$\operatorname{supp}(D) \cap \operatorname{supp}(E) = \emptyset,$$

where $E = D' + d/2 \operatorname{div}(x - \zeta)$. This corresponds to choosing $A = D_\infty$ and $A' = D_\zeta$ in the method outlined above, where $D_\zeta = \operatorname{div}(x - \zeta) + D_\infty$.

Instead of computing $\langle D, D \rangle$, we can now compute

$$\hat{h}(P) = -\langle D, D \rangle = \langle D, -D \rangle = \langle D, E \rangle.$$

If we have

$$D = \tilde{D} - \frac{d}{2} D_\infty,$$

where

$$\tilde{D} = \sum_{i=1}^{d'} (P_i) + n_\infty (\infty^+)$$

is reduced along $D_\infty = (\infty) + (\infty^-)$, such that $d = d' + n_\infty$ and all P_i are affine non-Weierstrass points (see Section 5.2.2), then we also have to move D away from ∞^+ using a function $x - \zeta'$, where $x(P_i) \neq \zeta' \neq \zeta$ for all $i = 1, \ldots, d'$. The computation becomes

$$-\langle D, D \rangle = \langle \sum_{i=1}^{d'} (P_i) + n_\infty (\infty^+) - \frac{d}{2} D_{\zeta'}, \sum_{i=1}^{d'} (P_i^-) + n_\infty (\infty^-) - \frac{d}{2} D_\zeta \rangle$$

and poses no additional problems due to the bilinearity of the local Néron symbol.

What if there is a unique rational Weierstrass point ∞ at infinity and d is odd? In that case we use

$$D' = 2 \sum_{i=1}^{d} (P_i^-) - d D_\infty \sim -2D$$

and compute

$$\hat{h}(P) = -\langle D, D \rangle = \langle D, -D \rangle = \frac{1}{2} \langle D, E \rangle,$$

where $E = D' + d \operatorname{div}(x - \zeta)$ and ζ is as above. Note that we can still use the reduced Mumford representation, because we have

$$\langle D, E \rangle = 2 \langle D, \sum_{i=1}^{d} (P_i^-) \rangle - d \langle D, D_\zeta \rangle.$$

Finally, if $\operatorname{supp}(D)$ contains an affine Weierstrass point, then we simply compute $\hat{h}(P) = \frac{1}{n^2} \hat{h}(nP)$ such that nP has a reduced representation not containing an affine Weierstrass point.

5.3.2 Determining relevant non-archimedean places

Given two divisors D and E with disjoint support, we have to find the finite set of non-archimedean places v such that $\langle D, E\rangle_v \neq 0$ is possible. Any such place must either be a place of bad reduction such that $D_{v,\mathcal{C}}$ and $E_{v,\mathcal{C}}$ intersect the singular locus of the closure $\mathcal{C}$ of C over $\mathrm{Spec}(\mathcal{O}_v)$ or we must have

$$i_v(D_{v,\mathcal{C}'}, E_{v,\mathcal{C}'}) > 0, \tag{5.3}$$

where $\xi : \mathcal{C}' \to \mathcal{C}$ is a desingularization of $\mathcal{C}$ in the strong sense (or both). Recall that ξ is a proper birational morphism with $\mathcal{C}'$ a regular model of C that is an isomorphism above regular points of $\mathcal{C}$. So (5.3) can only happen if the closures $D_{v,\mathcal{C}}$ and $E_{v,\mathcal{C}}$ do not have disjoint supports.

We can assume that D and E are effective and use their respective ideal representations. The idea is to cover our curve by affine patches $C^1, \ldots, C^n$ and determine the relevant places for each patch using Gröbner bases. See [1] for an introduction to the theory of Gröbner bases.

So let $C^i = \mathrm{Spec}\, k[x_1, \ldots, x_n]/(G_{i,1}(x_1, \ldots, x_n), \ldots, G_{i,m_i}(x_1, \ldots, x_n))$ be such an affine patch, where $G_{i,j}(x_1, \ldots, x_n) \in \mathcal{O}_k[x_1, \ldots, x_n]$ for all j. Suppose for now that the ring of integers $\mathcal{O}_k$ is Euclidean and that D and E are represented by ideals $I_{D,i}$ and $I_{E,i}$, respectively, on C^i for each i. In fact we can assume that $I_{D,i}$ and $I_{E,i}$ are given by bases whose elements are in $\mathcal{O}_k[x_1, \ldots, x_n]$. If we compute a Gröbner basis B_i of

$$I_{D,E,i} := (G_{i,1}(x_1, \ldots, x_n), \ldots, G_{i,n_m}(x_1, \ldots, x_n)) + I_{D,i} + I_{E,i}$$

over $\mathcal{O}_k$, then B_i contains a unique element $q_{D,E,i} \in \mathcal{O}_k$. By the above discussion, if (5.3) holds for some $v \in M_k^0$, then v must clearly satisfy $v(q_{D,E,i}) > 0$ for some i, so the problem comes down to factoring $q_{D,E,i}$ for all i. This can become quite time-consuming and in practice tends to be the most expensive part of the entire algorithm when some $q_{D,E,i}$ contains at least two large prime factors. If $v(q_{D,E,i}) > 0$, then we also know that we only have to do the local computations over the ring of integers $\mathcal{O}_v$ of the completion k_v modulo $\pi_v^{\mathrm{prec}_{D,E,v}}$, where π_v is a uniformizer at v and

$$\mathrm{prec}_{D,E,v} = \max\{v(q_{D,E,i}) : i \in \{1, \ldots, n\}\} + 1.$$

If $\mathcal{O}_k$ is not a Euclidean ring, then we can still use this Gröbner basis approach by writing k as $k'(\alpha)$, where k extends k' and the ring of integers $\mathcal{O}_{k'}$ of k' is Euclidean; for example we can use $k' = \mathbb{Q}$ in the number field case and $k' = l[x]$ in the function field case, where l is the constant field of k. This trick appears in [1, Exercise 4.3.1]. We add a new variable t to $\mathcal{O}_{k'}[x_1, \ldots, x_n]$, satisfying the relation

$$\phi_{k/k'}(t) = 0,$$

where $\phi_{k/k'}$ is the minimal polynomial of α over k', and replace any occurrence of α in $I_{D,E,i}$ by t. Now we get at most one $q_{D,E,i}(t) \in \mathcal{O}_{k'}[t] \setminus \mathcal{O}_{k'}$ in the Gröbner basis of $I_{D,E,i}$, but we might also have some $q'_{D,E,i} \in \mathcal{O}_{k'}$. We factor the principal ideal $q_{D,E,i}(\alpha)$ in $\mathcal{O}_k$ and, if necessary, the principal ideal $q'_{D,E,i}$ in $\mathcal{O}_k$ to find the relevant $v \in M_k^0$.

Applied to all affine patches C^i, the procedure introduced above finds all $v \in M_k^0$ such that $i_v(D_{v,\mathcal{C}'}, E_{v,\mathcal{C}'}) > 0$ is possible for a desingularization of the closure of the given model of C over $\mathrm{Spec}(\mathcal{O}_v)$ in the strong sense. For efficiency reasons we would like to keep the number of factorizations to a minimum. Suppose that C is covered by two affine patches C^1 and C^2. For instance, if C is a hyperelliptic curve given by a model of the form (5.2), then we can take

$$C^1 : y^2 + H(x,1)y = F(x,1) \tag{5.4}$$

and

$$C^2 : w^2 + H(1,z)w = F(1,z). \tag{5.5}$$

Suppose we have gone through the above-mentioned steps on C^1 and that the ideal representations of D and E on C^1 are $I_{D,1} = (a(x), cy - b(x))$ and $I_{E,1} = (a'(x), c'y - b'(x))$, respectively (where we have multiplied all polynomials by the common denominators of their coefficients, if necessary). Moreover suppose that $v \in M_k^0$ satisfies $i_v(D_{v,\mathcal{C}'}, E_{v,\mathcal{C}'}) > 0$, where $\mathcal{C}' \to \mathcal{C}$ is a desingularization in the strong sense over $\mathrm{Spec}(\mathcal{O}_v)$ and that the points of intersection do not lie above the closure of C^1. Any such v must satisfy $v(a_d) > 0$ and $v(a'_{d'}) > 0$, where a_d and $a'_{d'}$ are the leading coefficients of $a(x)$ and $a'(x)$, respectively.

These coefficients are usually much smaller than $q_{D,E,2}$ and so this simplification can make a big difference in practice. If we want to bound the precision that is necessary for the intersection computations, we can simply compute $q_{D,E,2}$ and $v(q_{D,E,2})$ for any such v (with the described modifications when $\mathcal{O}_k$ is not a Euclidean ring). Of course similar techniques can be applied in the case of smooth plane curves.

5.3.3 Regular models

In the following three sections we let R denote a discrete valuation ring with spectrum $S = \mathrm{Spec}(R)$, field of fractions l, valuation v, uniformizing element π and residue field $\mathfrak{l}$. Let C be a smooth projective geometrically connected curve of genus $g \geq 1$ defined over l and suppose that C is given by an R-integral model. Using a transformation, if necessary, We can assume that the closure $\mathcal{C}$ of the given model over S is normal and flat; therefore it has only isolated singularities on the special fiber.

The existence of a proper regular model $\mathcal{C}'$ of C over S is guaranteed by Theorem 1.20 which also gives a practical method of constructing such

a model. In fact, it always produces a desingularization of $\mathcal{C}$ in the strong sense; this property will turn out to be useful later on. As mentioned in Section 1.5, the construction of a proper regular model over S is implemented in `Magma` and hence we do not discuss it in any depth. This is always a desingularization of the closure $\mathcal{C}$ in the strong sense whenever this closure is normal and flat.

However, note that in the desingularization sequence (1.5) only the isolated singularities in the normal arithmetic surfaces $\mathcal{C}_i$ are blown up. In practice, one can often simplify this by blowing up an entire component that contains several singularities, because a blow-up is an isomorphism outside of the singular locus of its center, provided this locus is closed; see [17, Satz 1.29]. A regular model thus constructed still has the property that it is a desingularization of $\mathcal{C}$ in the strong sense. Note that this fact is already used in Tate's algorithm for the computation of a proper regular model of an elliptic curve, cf. [89, §IV.9]. Normalizations are usually more difficult than blow-ups from a computational point of view; a constructive method for computing normalizations is discussed in [56].

In the desingularization process one usually works over suitable affine charts as opposed to using the abstract Proj-construction as in [65, §8.1]. After resolving all singularities it is important, using the gluing maps stored along the way, to identify identical components in different affine charts, which essentially boils down to a bookkeeping issue.

5.3.4 Computing non-archimedean intersection multiplicities

We keep the notation from the previous section and assume, in addition, that C is covered by affine patches $C^1, \ldots, C^n$, where

$$C^i = \operatorname{Spec} l[x,y]/G_i(x,y)$$

and $G_i(x,y) \in R[x,y]$. This assumption is made for simplicity of presentation, but everything we do works in much greater generality. We stress our assumption that the closure $\mathcal{C}$ of the given model is normal and flat; it is covered by the affine patches

$$\mathcal{C}^i = \operatorname{Spec} R[x,y]/G_i(x,y).$$

In order to define intersection multiplicities in Section 5.1 we had to work on a regular model. In many cases, however, it is possible to work entirely on the closure $\mathcal{C}$ of the given model of C without any additional difficulty. Fix a desingularization $\xi : \mathcal{C}' \to \mathcal{C}$ in the strong sense and let $P, Q \in C(l)$. By definition, $i_v((P)_{\mathcal{C}'}, (Q)_{\mathcal{C}'}) > 0$ is only possible if the reductions $\tilde{P}$ and $\tilde{Q}$ on $\mathcal{C}_v = \tilde{C}$ are equal.

Now suppose we have two divisors D, E with disjoint support whose closures $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ have the property that their common support does not contain any singular points. Then, by the above, and because the total intersection is defined as a sum of local intersections, we might as well compute the intersection directly on the closure $\mathcal{C}$ of C over $\mathrm{Spec}(R)$ and this means that for the intersection computation we do not have to compute any regular model at all. By abuse of notation, we shall write $i_v(D_{\mathcal{C}}, E_{\mathcal{C}})$ in this situation when we mean in fact the intersection multiplicity $i_v(D_{\mathcal{C}'}, E_{\mathcal{C}'})$ on any desingularization $\mathcal{C}'$ of $\mathcal{C}$ in the strong sense.

For computational purposes we shall assume for the moment that we have two such divisors D and E whose closures over $\mathcal{C}$ lie entirely in an affine piece $\mathcal{C}^i$ for some $i \in \{1, \ldots, n\}$. The following lemma is very helpful in computations. It is a well-known result from commutative algebra saying that quotients and localizations commute.

Lemma 5.16. *Let A be a commutative ring with unity and let $T \subset A$ be a multiplicative subset. Let $I \subset A$ be an ideal and let $\bar{T}$ denote the image of T in A/I. Then we have*

$$A_T/IA_T \cong (A/IA)_{\bar{T}},$$

where the subscripts denote localizations.

Proof. See [69, Theorem 4.2]. □

We want to compute the intersection

$$i_v(D_{\mathcal{C}}, E_{\mathcal{C}}) = \sum_P i_P(D_{\mathcal{C}}, E_{\mathcal{C}})[\mathfrak{l}(P) : \mathfrak{l}],$$

where the sum is over all closed points of $\mathcal{C}_v^i$ lying in $\mathrm{supp}(D_{\mathcal{C}}) \cap \mathrm{supp}(E_{\mathcal{C}})$. In particular, no irregular points contribute toward the sum and hence the intersection takes place entirely on $\mathcal{C}^i$. Let l' be an extension of l such that all points in the support of D and E are defined over l' and let v' denote the extension of v to l'.

Lemma 5.17. *Suppose $D = \sum_i n_k(P_k)$ and $E = \sum_j m_j(Q_j)$, where P_k and Q_j are l'-rational and $n_k, m_j \in \mathbb{Z}$ for all k, j. Then we have*

$$i_v(D_{\mathcal{C}}, E_{\mathcal{C}}) = \sum_{k,j} n_k m_j \min\{v'(x(P_k) - x(Q_j)), v'(y(P_k) - y(Q_j))\},$$

where $P_k = (x(P_k), y(P_k)), Q_j = (x(Q_j), y(Q_j)) \in C^i$.

Proof. Using properties (a) and (g) of Proposition 5.7 we can assume that all P_k, Q_j lie in $C(l)$ and it suffices to compute $i_P((P_k)_{\mathcal{C}}, (Q_j))_{\mathcal{C}}$ for some P_k, Q_j and $P \in \mathcal{C}_v^i$. We can also assume that $P_k \equiv P \pmod{\pi}$ and $Q_j \equiv P$

(mod π), since otherwise the intersection is zero. The remainder of this proof is similar to calculations done by Busch in [17] in order to compute intersection multiplicities in the case of elliptic curves. According to Definition 1.29 we get

$$i_P((P_k)_{\mathcal{C}}, (Q_j)_{\mathcal{C}}) = \text{length}_{\mathcal{O}_{\mathcal{C}^i,P}} \mathcal{O}_{\mathcal{C}^i,P}/(I_{(P_k),i} + I_{(Q_j),i}).$$

We have

$$\mathcal{O}_{\mathcal{C}^i,P} = (R[x,y]/G_i(x,y))_{\mathfrak{m}_P},$$

where $\mathfrak{m}_P = (x - x(P), y - y(P), \pi)$ is the maximal ideal at P. The defining ideals of $(P_k)_{\mathcal{C}}$ and $(Q_j)_{\mathcal{C}}$ in $\mathcal{O}_{\mathcal{C}^i,P}$ are given by

$$I_{(P_k),i} = (x - x(P_k), y - y(P_k))$$

and

$$I_{(Q_j),i} = (x - x(Q_j), y - y(Q_j)).$$

Therefore we find

$$\begin{aligned}
&\mathcal{O}_{\mathcal{C}^i,P}/(I_{(P_k),i} + I_{(Q_j),i}) \\
&\cong (R[x,y]/G_i(x,y))_{\mathfrak{m}_P} /(x - x(P_k), y - y(P_k), x - x(Q_j), y - y(Q_j)) \\
&\cong (R[x,y]/(G_i(x,y), x - x(P_k), y - y(P_k), x - x(Q_j), y - y(Q_j)))_{\mathfrak{m}_P},
\end{aligned}$$

where the second isomorphism follows from Lemma 5.16. Now we apply the morphisms $x \mapsto x(P_k)$ and $y \mapsto y(P_k)$ and obtain

$$\begin{aligned}
\mathcal{O}_{\mathcal{C}^i,P}/(I_{(P_k),i} + I_{(Q_j),i}) &\cong R_{(\pi)}/(x(P_k) - x(Q_j), y(P_k) - y(Q_j))R_{(\pi)} \\
&\cong R/(x(P_k) - x(Q_j), y(P_k) - y(Q_j))R
\end{aligned}$$

from which the result follows.

□

In [50] Holmes also states Lemma 5.17 independently for hyperelliptic curves of odd degree without proof. He then proceeds to express the right hand side in terms of certain resultants that are easily computable over the ground field l. This only works for hyperelliptic curves. We describe a different approach that applies to more general curves. For simplicity we suppose, in addition to our previous assumptions, that the special fiber $\mathcal{C}_v$ is irreducible as a divisor on $\mathcal{C}$. Moreover, we assume that the defining ideals $I_{D,i}$ and $I_{E,i}$ of D and E, respectively, are given by bases consisting of polynomials with coefficients in R. Hence they are also defining ideals of $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$.

For the computation of the intersection multiplicity we use the following version of the Chinese remainder theorem for modules.

Proposition 5.18. *Let A be a commutative ring and let M be an Artinian and Noetherian A-module. Then there is an isomorphism of A-modules*

$$M \cong \bigoplus_P M_P,$$

where the sum is over all maximal ideals P of A and M_P denotes the localization of M at P.

Proof. See [36, Theorem 2.13]. □

We use this result to express $i_v(D_\mathcal{C}, E_\mathcal{C})$ as the length of an $\mathcal{O}_{\mathcal{C}_v}$-module, where we view $\mathcal{C}_v$ as a prime divisor on $\mathcal{C}$. It follows from our assumptions that we may restrict to

$$\mathcal{C}_v^i = \operatorname{Spec} \mathfrak{l}[x,y]/\tilde{G}_i(x,y),$$

where $\tilde{G}_i(x,y)$ is the reduction of $G(x,y)$ modulo π. The maximal ideal at the generic point of $\mathcal{C}_v$ is the maximal ideal (π) of R, and so the local ring is

$$\mathcal{O}_{\mathcal{C}_v^i} = \left(R[x,y]/G_i(x,y)\right)_{(\pi)}.$$

Proposition 5.19. *We have*

$$i_v(D_\mathcal{C}, E_\mathcal{C}) = \operatorname{length}_{\mathcal{O}_{\mathcal{C}_v^i}} \left(\mathcal{O}_{\mathcal{C}_v^i}/(I_{D,i} + I_{E,i})\mathcal{O}_{\mathcal{C}_v^i}\right)$$

Proof. From Proposition 5.18 we get an isomorphism of $\mathcal{O}_{\mathcal{C}_v^i}$-modules

$$\mathcal{O}_{\mathcal{C}_v^i}/(I_{D,i} + I_{E,i}) \cong \sum_P \mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i}), \tag{5.6}$$

where the sum is over all maximal ideals of $\mathcal{O}_{\mathcal{C}_v^i}$, that is, over all closed points $P \in \mathcal{C}_v^i$. By our assumptions we have

$$\begin{aligned}
i_v(D_\mathcal{C}, E_\mathcal{C}) &= \sum_P i_P(D_\mathcal{C}, E_\mathcal{C})[\mathfrak{l}(P) : \mathfrak{l}] \\
&= \sum_P \operatorname{length}_{\mathcal{O}_{\mathcal{C}^i,P}} \left(\mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i})\right)[\mathfrak{l}(P) : \mathfrak{l}] \\
&= \sum_P \operatorname{length}_{\mathcal{O}_{\mathcal{C}_v^i}} \left(\mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i})\right) \\
&= \operatorname{length}_{\mathcal{O}_{\mathcal{C}_v^i}} \bigoplus_P \left(\mathcal{O}_{\mathcal{C}^i,P}/(I_{D,i} + I_{E,i})\right) \\
&= \operatorname{length}_{\mathcal{O}_{\mathcal{C}_v^i}} \left(\mathcal{O}_{\mathcal{C}_v^i}/(I_{D,i} + I_{E,i})\right)
\end{aligned}$$

using (5.6), additivity of the length and the fact that if M is an $\mathcal{O}_{\mathcal{C}_v^i}$-module that is also an $\mathcal{O}_{\mathcal{C}^i,P}$-module for some closed point $P \in \mathcal{C}_v^i$, then we have

$$\operatorname{length}_{\mathcal{O}_{\mathcal{C}_v^i}}(M) = \operatorname{length}_{\mathcal{O}_{\mathcal{C}^i,P}}(M)[\mathfrak{l}(P) : \mathfrak{l}].$$

□

We can explicitly construct the R-algebra

$$A_{D,E,i,v} := (R[x,y]/I_{D,E,i,v})_{(\pi)} \cong \mathcal{O}_{\mathcal{C}_v^i}/(I_{D,i} + I_{E,i}), \tag{5.7}$$

where

$$I_{D,E,i,v} = (G_i(x,y)) + I_{D,i} + I_{E,i}, \tag{5.8}$$

using Lemma 5.16.

The computation of $\text{length}_{\mathcal{O}_{\mathcal{C}_v^i}} A_{D,E,i,v}$ is rather easy and can be done, for instance, in `Magma`. See Algorithm 3 which is also applicable for any number of variables. The crucial step is the computation of a Gröbner basis B of $I_{D,E,i,v}$ over the Euclidean ring R, which is usually very fast because the ideal is zero-dimensional and the polynomials involved have quite low degree. We will return to this question later on in Section 6.2.1. We refer to [1, Chapter 4] for an introduction to the theory and applications of Gröbner bases for polynomial rings over Euclidean rings. What we need here is that all polynomials h in $R[x,y]$ have a well-defined remainder h mod B.

Algorithm 3 Computation of $\text{length}_{\mathcal{O}_{\mathcal{C}_v^i}} A_{D,E,i,v}$

$B = \{g_1(x,y), \ldots, g_r(x,y), q\} \leftarrow$ Gröbner basis of $I_{D,E,i,v}$
$m \leftarrow v(q)$
$td \leftarrow 0$
$T \leftarrow \emptyset$
repeat
  $td \leftarrow td + 1$
  $V \leftarrow \{x^i y^j : i + j = td \text{ and } \nexists h \in T \text{ such that } h \mid x^i y^j\}$
  $m' \leftarrow m$
  for $g \in V$ **do**
    $n \leftarrow 0$
    while $\deg(\pi^n g \bmod B) > td$ or $g \mid \pi^n g \bmod B$ **do**
      $n \leftarrow n + 1$
    end while
    $m \leftarrow n + m.$
    if $n = 0$ **then**
      $T \leftarrow T \cup \{g\}$
    end if
  end for
until $m = m'$
return m

In the course of this section we have made several simplifying assumptions:

(a) The respective closures $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ lie entirely in a single affine piece $\mathcal{C}^i$.

(b) The ideals $I_{D,i}$ and $I_{E,i}$ are given by R-integral bases.

(c) The special fiber $\mathcal{C}_v$ is irreducible.

(d) The closures $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ contain no irregular point.

(e) The affine piece C^i is given by $\operatorname{Spec} k[x,y]/G_i(x,y)$.

Note that assumption (b) implies assumption (a). Assumption (e) is completely unnecessary for everything we did in this chapter, but simplified the exposition. We will deal with divisors that do not satisfy (d) below.

Suppose we want to apply Lemma 5.17 or Proposition 5.19 and we are given an effective divisor $D \in \operatorname{Div}(C)(l)$ such that assumption (b) above does not hold for any affine piece C^i. Then we need to decompose D into $D = \sum_{j=1}^{n} D_j$ such that all $D_{j,\mathcal{C}}$ lie completely in some $\mathcal{C}^{i_j}$ and furthermore we have an R-integral basis for each $I_{D_j,i}$. In order to accomplish this it is not strictly necessary to decompose D into prime divisors, but it is certainly the most straightforward approach. Because R is Henselian, any prime divisor must reduce completely to a single affine patch and so (a) holds, although a field extension may be required to satisfy (b).

In order to decompose divisors one uses the ideal representation and for this one needs to compute the factorization of multivariate polynomials as in [48]. But currently this is not implemented over local fields in `Magma` and so we cannot always use this approach. Of course, if C is defined over a number field or one-dimensional function field k, where $l = k_v$, and we already have a decomposition of D and E over k such that (a) and (b) hold for the respective summands, then we can simply apply Proposition 5.19 to these summands.

So we can always compute canonical heights over an extension field k'/k over which we can decompose D and E into divisors for which (a) and (b) hold for the localizations at every v. This may require a rather large extension.

We discuss the situation for hyperelliptic curves next; here we can decompose divisors easily, because this reduces to factorization of univariate polynomials over l and this is implemented in `Magma`, at least when l is the completion of a global field. The techniques described below are thus applicable whenever decompositions of divisors can be determined using factorization of univariate polynomials. A possible approach to the problem of representing divisors on smooth plane quartics that closely resembles Mumford representations of divisors on hyperelliptic curves and may thus be useful for the computation of canonical heights is presented in [83].

Finally a word on assumption (c): This is unnecessary, provided that points in the common support of $D_{\mathcal{C}}$ and $E_{\mathcal{C}}$ all lie on the same irreducible component of the special fiber. If this is satisfied, we can simply use the local ring of the relevant component, since in practice this ring is rather easy to compute. If not, then we have to work over a suitable extension as usual.

An example of a situation that allows us to compute non-archimedean intersections using Proposition 5.19 is the case of hyperelliptic curves. Suppose the affine pieces C^1 and C^2 covering C are defined as in (5.4) and (5.5) and suppose, for simplicity, that the special fiber $\mathcal{C}_v$ of the closure is irreducible. Let $D \in \mathrm{Div}(C)(l)$ be effective such that its ideal representation is

$$I_{D,1} = (a(x), y - b(x)),$$

where $a(x), b(x) \in l[x]$ and we have $\deg(a) \leq g$ and $\deg(b) \leq g + 1$ as in Section 5.2.2. We can factor $a(x) = a_1(x)a_2(x)$, where $a_2(x)$ is constant modulo π and $a_1(x) \in R[x]$. This corresponds to a decomposition $D = D_1 + D_2$, where $D_{1,\mathcal{C}}$ lies in $\mathcal{C}^1$ and $D_{2,\mathcal{C}}$ lies in $\mathcal{C}^2$. More precisely, we have

$$I_{D_1,1} = (a_1(x), y - b_1(x)),$$

where $b_1(x) = b(x) \pmod{a_1(x)}$. In order to use Proposition 5.19, we need $b_1(x) \in R[x]$, but if this does not hold we can extend the field l, and thus we assume that this is satisfied. In practice the case that such an extension is necessary does not seem to occur often. We also get

$$I_{D_2,1} = (a_2(x), y - b_2(x))$$

where $b_2(x) = b(x) \pmod{a_2(x)}$, although we are of course more interested in the defining ideal $I_{D_2,2}$, but the latter can be determined using the same method. This way we can obtain the desired decomposition into divisors satisfying (a) and (b) above.

Hence we can assume that D and E are effective divisors with disjoint support satisfying (a), (b) and (d) for $i = 1$ and we have

$$I_{D,1} = (a(x), y - b(x))$$

and

$$I_{E,1} = (a'(x), y - b'(x)).$$

Then

$$I_{D,E,1,v} = (y^2 + H(x,1)y - F(x,1), a(x), y - b(x), a'(x), y - b'(x))$$

is the ideal defined in (5.8) that we need to compute a Gröbner basis of.

It is now straightforward to apply Proposition 5.19 using Mumford representations. Note that according to Section 5.3.1 some of the divisors we encounter have an ideal representation of the form $I_{D,1} = (x - \zeta)$ and that makes the Gröbner basis computations even easier. In practice the algorithm outlined above has proved faster than the resultants method due to Holmes in all examples considered so far.

Up to now we have assumed that all intersections take place at regular points on the closure $\mathcal{C}$ of C over S. Now let $D, E \in \mathrm{Div}(C)(l)$ with disjoint support such that $\mathrm{supp}(D_{\mathcal{C}}) \cap \mathrm{supp}(E_{\mathcal{C}})$ includes irregular points of $\mathcal{C}_v$. Suppose

$$D = \sum_i (P_i), \quad E = \sum_j (Q_j) \tag{5.9}$$

and that $\mathrm{supp}(D_{\mathcal{C}})$ and $\mathrm{supp}(E_{\mathcal{C}})$ both lie in the same affine piece $\mathcal{C}^i$. Let $\mathcal{C}'$ denote a desingularization in the strong sense of $\mathcal{C}$ over S.

We want to compute $i_v(D_{\mathcal{C}'}, E_{\mathcal{C}'})$. If we can compute the decompositions (5.9), then we can look for an affine piece $\mathcal{C}'_{i,j}$ of the generic fiber of $\mathcal{C}'$ containing images of the points P_i and Q_j for each i and j and compute the intersection using a formula similar to Lemma 5.17. We determine the images of P_i and Q_j on $\mathcal{C}'_v$ by following through the construction of $\mathcal{C}'$. If no such affine piece exists, then the intersection of $(P_i)_{\mathcal{C}'}$ and $(Q_j)_{\mathcal{C}'}$ must be trivial. This approach requires extending the ground field to some $l_{i,j}$ such that both P_i and Q_j are defined over $l_{i,j}$.

Fortunately we can sometimes do better. Since the blow-ups and normalizations used to construct $\mathcal{C}'$ induce transformations between the different affine pieces covering $\mathcal{C}'$, it is natural to investigate how these transformations act on the defining ideals of D and E. If the curve is hyperelliptic, for instance, they act on the Mumford representation. Hence we can sometimes work entirely over the ground field.

We illustrate this in the simplest case. We treat the uniformizer π as a variable. Suppose we need to blow up a closed point $P \in \mathcal{C}^i_v$ on the special fiber. We may assume without loss of generality that it is l-rational, because otherwise the desingularization process (for example as implemented in `Magma`) uses an extension l' of l such that P is defined over the residue class field of l' and this forces us to work over l' anyway. Using a transformation, we can assume P is at $x = 0, y = 0, \pi = 0$, so we are in the classical situation of blowing up the origin of affine 3-space containing $\mathcal{C}^i_v$, that is, we introduce new variables x_1, y_1, π_1 satisfying

$$xy_1 = yx_1, x\pi_1 = \pi x_1, y\pi_1 = \pi y_1.$$

This leads to three affine charts $\mathcal{C}_1 = \{x_1 \neq 0\}, \mathcal{C}_2 = \{y_1 \neq 0\}, \mathcal{C}_3 = \{\pi_1 \neq 0\}$ covering the blow-up and three transformations $\tau_i : \mathcal{C} \longrightarrow \mathcal{C}_i$ acting on affine points by

$$\begin{aligned} \tau_1(x, y, \pi) &= (x, y_1, \pi_1) = (x, y/x, \pi/x), \\ \tau_2(x, y, \pi) &= (x_1, y, \pi_1) = (x/y, y, \pi/y), \\ \tau_3(x, y, \pi) &= (x_1, y_1, \pi) = (x/\pi, y/\pi, \pi). \end{aligned}$$

Suppose that C is hyperelliptic, D is an effective divisor of degree $d \geq 0$ whose support does not contain a point at infinity and $I_{D,1} = (a(x), y - b(x))$.

Since $P = (0,0,0) \in \mathcal{C}_v(\mathfrak{l})$, we know that the reduction $\tilde{a}(x)$ factors as

$$\tilde{a}(x) = x^m g(x),$$

where $m \geq 0$ and $g(x) \in \mathfrak{l}[x]$ is such that $g(0) \neq 0$. Similarly, we have

$$\tilde{a'}(x) = x^{m'} g'(x),$$

where $m' \geq 0$, $g'(x) \in \mathfrak{l}[x]$ is such that $g'(0) \neq 0$ and $I_{E,i} = (a'(x), y - b'(x))$. Hence we know that m of the P_i and m' of the Q_j reduce to P and therefore lie on one of the components contracted to P under the blow-up map.

The action of the transformations is given by

$$\begin{aligned} I_{\tau_1^*(D),1} &= (a(x), xy_1 - b(x), \pi - \pi_1 x), \\ I_{\tau_2^*(D),1} &= (a(x_1 y)/y^2, y - b(x_1 y), \pi - \pi_1 y), \\ I_{\tau_3^*(D),1} &= (a(\pi x_1)/\pi^2, y_1 - b(x_1)/\pi), \end{aligned}$$

and similarly for $(a'(x), y - b'(x))$. After applying the transformations, we can check easily how many P_i and Q_j reducing to P become regular and which components they map to. If all points map to regular points, then we compute the intersections on the respective affine charts using Proposition 5.19, otherwise we continue this process.

If both $a(x)$ and $a'(x)$ happen to be unramified, then we are in the particularly convenient situation that the entire intersection takes place on the third affine chart $\mathcal{C}_3$ defined by $\pi_1 \neq 0$, as all P_i and Q_j reducing to P map to this chart. Since the transformation τ_3 is given by

$$(x, y, \pi) \mapsto (x/\pi, y/\pi, \pi),$$

we have

$$i_v((\tau_3(P_i))_{\mathcal{C}_1}, (\tau_3(Q_j))_{\mathcal{C}_1}) = i'_v(P_i, Q_j) - 1, \tag{5.10}$$

where

$$i'_v(P_i, Q_j) = \min\{v(x(P_i) - x(Q_j)), v(y(P_i) - y(Q_j))\}.$$

Therefore we are not actually required to apply τ_3; it is sufficient to compute how many P_i and Q_j map to P. We can iterate this process, so in case only points have to be blown up in order to construct $\mathcal{C}'$ (for instance, when $\mathcal{C}$ has rational singularities), we can compute the intersection multiplicity entirely on $\mathcal{C}$, followed by subtraction of a certain integer which we can calculate as above by tracing through the blow-up process.

If we have to normalize in the desingularization process, more complications arise. If we can get away with blowing up a line, then we can again assume that it is $\mathfrak{l}$-rational. Hence we can compute the preimages under the blow-up map entirely using the ideal representation just as above. However, it is not possible any longer to compute the intersection multiplicity on $\mathcal{C}_v$

when $a(x)$ and $a'(x)$ are unramified because there is no useful analog of (5.10). In this case, it might be more suitable to employ Holmes' algorithm that uses resultants, see [50], since, in contrast with our algorithm, it does distinguish between contributions coming from differences of x-coordinates and those coming from differences of y-coordinates.

We have not investigated the case of more general normalizations. However, since in practice one usually performs such normalizations purely on the level of rings (see [56]), it should be possible to obtain further simplifications.

In [50] Holmes introduces a different method for the computation of $\langle D, E\rangle_v$ when $\mathrm{supp}(D_{\mathcal{C}}) \cap \mathrm{supp}(E_{\mathcal{C}})$ includes irregular points, at least in the case of models of the form $y^2 = f(x)$, where $f(x)$ is monic of odd degree. He proves that we have

$$\langle D, E\rangle_v = \langle \mathrm{div}(h), E\rangle_v + i_v(D'_{\mathcal{C}}, E_{\mathcal{C}})$$

whenever $h \in l(C)^*$ is such that $D' = D - \mathrm{div}(h)$ and E have disjoint support and that $D'_{\mathcal{C}}$ contains no irregular points. The question is whether such an h can always be found. This is answered affirmatively in [50] if we allow taking multiples of D and E. However, we have found that our approach outlined above has been more efficient in all examples considered so far.

On a side note, an important application of canonical heights consists of the gathering of numerical evidence for the Birch and Swinnerton-Dyer conjecture on abelian varieties as in [44]. See also Section 1.7. In order to do this, we also need to compute the Tamagawa numbers for all non-archimedean places v and this requires computing regular models at these places, so for this application we can assume a priori that such models are available. Moreover, the recent work [51] of Holmes, where a good candidate for the naive height is constructed, also uses the minimal regular model.

5.3.5 Computing the correction term

We continue to let $\mathcal{C}'$ denote a desingularization in the strong sense of $\mathcal{C}$ over S, where the closure $\mathcal{C}$ of C over S is assumed normal and flat. Suppose that the special fiber $\mathcal{C}'_v$ is equal to $\sum_{i=0}^{r} n_i \Gamma_v^i$, where $\Gamma_v^0, \ldots, \Gamma_v^r$ are the irreducible components of $\mathcal{C}'_v$. Let M_v be the intersection matrix $\left(i_v(n_i\Gamma_v^i, n_j\Gamma_v^j)\right)_{0\le i,j\le r}$ of $\mathcal{C}'_v$ as in Lemma 5.1.

Suppose we are given a divisor $D \in \mathrm{Div}^0(C)(l)$ and we want to compute a representative $\sum_{i=0}^{r} \alpha_i n_i \Gamma_v^i$ of $\Phi_{v,\mathcal{C}'}(D)$. For this we can use the proof of Lemma 5.1, provided we have found both M_v and $s(D)$, where

$$s(D) = \left(n_0 i_v(D_{\mathcal{C}'}, \Gamma_v^0), \ldots, n_r i_v(D_{\mathcal{C}'}, \Gamma_v^r)\right)^T. \tag{5.11}$$

We mention two possible methods here.

(i) Let M_v^+ be the Moore-Penrose pseudoinverse of M_v. Then setting

$$(\alpha_0, \ldots, \alpha_r)^T := -M_v^+ s(D)^T$$

works.

(ii) (Cox-Zucker) Suppose that there exists some i such that $n_i = 1$, say $n_0 = 1$, and let M_v' be the matrix obtained by deleting the first column and row from M_v. Then setting $\alpha_0 := 0$ and

$$(\alpha_1, \ldots, \alpha_r)^T := -M_v'^{-1} s'(D)$$

works, where $s'(D)$ is the vector obtained by removing the first entry of $s(D)$. See [26].

Note that the first method always works, whereas the second method requires a familiar condition to be satisfied. As usual, if C has an l-rational point, then we have nothing to worry about.

We can now compute $i_v(\Phi_{v,\mathcal{C}'}(D), E_{\mathcal{C}'})$ easily for $E \in \mathrm{Div}^0(C)(l)$ having support disjoint from D. This is simply equal to

$$s(E)^T(\alpha_0, \ldots, \alpha_r),$$

where $s(E)$ is defined as in (5.11).

We still have to discuss how $s(D)$ and $s(E)$ can be computed. But this is already contained in the previous section. We can decompose D and E into prime divisors of degree 1, possibly over a finite extension of l, and then determine which components the corresponding points map to by tracing through the blow-up (respectively normalization) process. In favorable situations (for instance in the case of hyperelliptic curves) we can work with the ideal representations of D and E, see the discussion in the previous section.

5.3.6 Computing archimedean intersection multiplicities

In this section we fix an archimedean place $v \in M_k^\infty$. Our main reference is [59, Chapter 13]. Suppose that we have embedded C into $\mathbb{P}^N_{\mathbb{C}}$ for some N using v and let $C(\mathbb{C})$ denote the associated Riemann surface. According to Section 5.2 we need to find an almost-Green's function with respect to a divisor $D \in \mathrm{Div}^0(C)(\mathbb{C})$. Notice that we can write any such divisor in the form $D = D_1 - D_2$, where D_1 and D_2 are *non-special*, that is they are effective of degree g and their $\mathcal{L}$-spaces have dimension 1. By additivity of Green's functions it suffices to determine almost-Green's functions with respect to non-special divisors and any fixed normalized volume form on $C(\mathbb{C})$.

In order to do this it turns out to be useful to work on the analytic Jacobian J. Recall the notation introduced in Section 1.6. We view J as an abelian variety over the complex numbers embedded using v. Let $\tau_v \in \mathfrak{h}_g$ such that $J(\mathbb{C})$ is isomorphic to $\mathbb{C}^g/\Lambda_v$, where $\Lambda_v = \mathbb{Z}^g \oplus \tau_v\mathbb{Z}^g$. Let the map j be defined by

$$j : \mathbb{C}^g \longrightarrow\!\!\!\!\!\rightarrow \mathbb{C}^g/\Lambda_v \xrightarrow{\cong} J(\mathbb{C}).$$

Moreover, we fix an Abel-Jacobi map, that is an embedding ι, defined over $\mathbb{C}$, of the curve into its Jacobian and let $\Theta \in \mathrm{Div}(J)$ denote the theta-divisor with respect to ι. Let $S : \mathrm{Div}(C) \longrightarrow J$ denote the summation map associated to ι.

On $J(\mathbb{C})$ we can find the following canonical 2-form: Let $\eta_1, \ldots, \eta_g$ be an orthonormal basis of the differentials of first kind on the Jacobian. Then the canonical 2-form is given by

$$\frac{1}{2g}(\eta_1 \wedge \bar{\eta}_1 + \ldots + \eta_g \wedge \bar{\eta}_g)$$

and we define the *canonical volume form* $d\mu$ *on* $C(\mathbb{C})$ by pulling this form back using ι, see [59, §13.2]. The details are not important for us as the dependence on $d\mu$ disappears because we only want to compute almost-Green's functions with respect to divisors of degree zero.

For the next theorem, conjectured by Arakelov and proved by Hriljac, recall the definition of Néron functions from Section 1.3. We use the notation E_P to denote the translation of a divisor $E \in \mathrm{Div}(J)$ by a point $P \in J$.

Theorem 5.20. *(Hriljac) Let $D \in \mathrm{Div}^g(C)$ be non-special, let $P = S(D)$ and $D' = ([-1]^*(\Theta))_P$. Let $\lambda_{D',v}$ be a Néron function with respect to D' and v. Then $\lambda_{D'} \circ \iota$ is an almost-Green's function with respect to D and $d\mu$, where $d\mu$ is the canonical volume form on $\mathcal{C}_v(\mathbb{C})$*

Proof. See [59, Chapter 13, Theorem 5.2]. □

Remark 5.21. Additivity of Green's functions and Theorem 5.20 can be combined to give a proof of the existence of Green's functions for any $D \in \mathrm{Div}(C)$ with respect to $d\mu$, and hence, using [60, Proposition 1.3] with respect to *any* normalized volume form. See [59, Chapter 13, Theorem 5.1].

The great news is that we already know how to find Néron functions with respect to Θ in the case of an archimedean place; we show below that this suffices for our purposes. Recall Proposition 4.15, stating that the function

$$\lambda'_{\Theta,v}(P) = -\log|\theta_{a,b}(z(P))|_v + \pi\,\mathrm{Im}(z(P))^T(\mathrm{Im}(\tau_v))^{-1}\,\mathrm{Im}(z(P))$$

is a Néron function associated with Θ and v, where $a = (1/2, \ldots, 1/2), b = (g/2, (g-1)/2, \ldots, 1, 1/2) \in \mathbb{C}^g$ and $\theta_{a,b}$ denotes the theta function with characteristic $[a; b]$ defined in Section 1.6. Now suppose that $D = D_1 - D_2$,

where $D_1, D_2 \in \mathrm{Div}(C)$ are non-special divisors with disjoint support, and let $E_1 = \sum_{i=1}^{d}(P_i)$ and $E_2 = \sum_{i=1}^{d}(Q_i)$ be two effective divisors such that $\mathrm{supp}(E_i) \cap \mathrm{supp}(D_j) = \emptyset$ for $i, j \in \{1, 2\}$.

Corollary 5.22. *We have*

$$\begin{aligned}
&\langle D_1 - D_2, E_1 - E_2 \rangle_v \\
&= -\log \prod_{i=1}^{d} \frac{|\theta_{a,b}(z(\iota(P_i)) - z(S(D_1)))\theta_{a,b}(z(\iota(Q_i)) - z(S(D_2)))|}{|\theta_{a,b}(z(\iota(P_i)) - z(S(D_2)))\theta_{a,b}(z(\iota(Q_i)) - z(S(D_1)))|} \\
&\quad - 2\pi \sum_{i=1}^{d} \mathrm{Im}(z(S(D_1) - S(D_2)))^T \,\mathrm{Im}(\tau_v)^{-1}\, \mathrm{Im}(z(\iota(P_i)) - z(\iota(Q_i))),
\end{aligned}$$

where for any $Q \in J$ the vector $z(Q) \in \mathbb{C}^g$ satisfies $j(z(Q)) = Q$.

Proof. Néron functions are invariant under translation of the divisor up to an additive constant, see [59, Chapter 11, Theorem 2.1]. But according to [59, Chapter 5, Theorem 5.8], $[-1]^*(\Theta)$ is just Θ translated by $S(\mathfrak{K})$, where $\mathfrak{K}$ is a canonical divisor. Hence the desired result follows from Theorem 5.20 and Proposition 4.15. □

Remark 5.23. In [50] Holmes gives a more direct proof of Lemma 5.22 using [59, §13.6/7], which relies on the theory of differentials of third kind.

We can use the previous result to compute intersections at archimedean places. In practice we need to be able to do the following:

1) Given $D \in \mathrm{Div}^0(C)$, find non-special D_1, D_2 such that $D = D_1 - D_2$.

2) Compute the period matrix τ_v.

3) Given $P_1 \in C(\mathbb{C})$ and τ_v, determine $z \in \mathbb{C}^g$ such that $j(z) = \iota(P_1)$.

4) Given τ_v and $z \in \mathbb{C}^g$, compute $\theta_{a,b}(z) = \theta_{a,b}(z, \tau_v)$.

The first step is not difficult, because we can, if need be, compute multiples of our divisor and use the bilinearity of the local Néron symbol. For hyperelliptic curves, steps 2), 3) and 4) are all implemented in `Magma` by van Wamelen, as already mentioned in Section 3.7.2. In the general case all of the relevant algorithms have been developed (see [29], [7] and [30]) by Deconinck et al. Both approaches are essentially numerical in nature. In contrast to the non-archimedean case the running times of steps 2), 3) and 4) do not crucially depend on the heights of the points in the supports of the respective divisors, since we work with the complex uniformisation. But the amount of work required to find the image of a point $P_1 \in C$ on the Riemann surface $C(\mathbb{C})$ does depend on this height.

For computational purposes, we want to stress that only D_1 and D_2 are required to be of degree g; E_1 and E_2 can be effective of lower degree. In

many situations the divisor E which we start with is given in such a form, for instance $E_1 = (P_1)$ and $E_2 = (Q_1)$, where $P_1, Q_1 \in C$. Moreover, it is actually desirable to work with E_i of low degree, because this means fewer applications of the Abel-Jacobi map ι and of theta functions are necessary, significantly reducing the running time of the entire algorithm.

Remark 5.24. Deconinck and his collaborators have implemented their algorithms in `Maple` in a package called *algcurves*. Their approach requires the curve to be given as an affine plane curve in $\mathbb{A}^2$, but because their algorithm can deal with singular Riemann surfaces, this is not an essential restriction. Since version 11 of `Maple`, this package has been part of the official `Maple` distributions. Unfortunately, the `Maple` developers have since decided to change some of the functions that algcurves uses, in the process destroying some of the package's functionality. For instance, the implementation of the Abel-Jacobi map is now very unreliable and only occasionally returns the correct value (if indeed it returns anything at all).

This means that the package, which worked perfectly well for `Maple` 10, is now useless for our purposes. Deconinck [31] is currently working on a long-term project to rewrite all necessary routines in `Sage` [91]. Once this is completed, steps 1) – 4) should again be possible and we can compute canonical heights on non-hyperelliptic Jacobians in practice. For the moment, however, this is limited to hyperelliptic Jacobians.

Chapter 6

Examples and timings

In this final chapter we investigate how the algorithms developed in this thesis can be applied in practice.

6.1 Jacobian surfaces

We start by discussing practical implications of Chapter 3. Let k be a number field or a one dimensional function field. If J is the Jacobian of a genus 2 curve C, then we can use our algorithm introduced in Chapter 3 for the computation of canonical heights on J and we can also use our results from that chapter to obtain better bounds on the non-archimedean local height constants than those that were previously available.

6.1.1 Computing heights

We briefly discuss the advantages and disadvantages of our algorithm for the computation of canonical heights on Jacobian surfaces introduced in Chapter 3. We first note that a comparison to the current `Magma`-implementation of the algorithm of Flynn, Smart and Stoll (see Sections 3.2.2 and 3.2.3) is not very useful, because that implementation is not optimized; it uses global arithmetic instead of v-adic arithmetic which would speed up the computations significantly.

The main advantage of our algorithm is that for the computation of the values of the error function $\mu_v(P)$, where $P \in J(k)$ and $v \in M_k^0$, we usually do not have to compute multiples of points on the Jacobian or on the Kummer surface. In those cases where we do have to compute multiples nP the number n can only be larger than 4 if we have reduction type $[I_{m_1} - I_{m_2} - l]$, where $m_1, m_2 > 4$ and $l > 1$ and this case can only occur when $v(\Delta(C)) > 22$, where $\Delta(C)$ is the discriminant of the curve C. Furthermore, our algorithm works for non-global one dimensional function fields (as always, with perfect residue fields), see Remark 3.75.

Suppose that k is a global field, so that the algorithm due to Flynn, Smart and Stoll is guaranteed to work theoretically. It is easy to find examples where the current implementation fails or becomes very time consuming. This happens whenever one of the integers M_v becomes large, where for a non-archimedean place $v \in M_k$, M_v is the smallest positive integers such that $\varepsilon_v(M_v P) = 0$. The size of the coordinates of $\kappa(nP)$ grows at a rate of about n^2 if we work over a global field and since we have to compute $\kappa(2M_v P)$, this can become prohibitive. See the introduction of [94] for an example. If we are in one of the five cases for which we have explicit formulas, then we can usually bound the number M_v explicitly. Recall that when the model is semistable we have rational singularities and hence ε_v factors

through the component group Φ_v.

- Suppose C has reduction type $[I_{m-0-0}]$ (see Section 3.6.1), where $m = v(\Delta)$ is large. Then the largest M_v that we can have is $M_v = m$. For a curve with reasonably small coefficients, it is therefore unlikely that M_v becomes too large for the current implementation.

- The situation for reduction type $[I_{m_1-m_2-0}]$ discussed in Section 3.6.2 can be worse, because we have $v(\Delta) = m_1 + m_2$, but we may need $M_v = m_1 m_2$, since $\Phi_v \cong \mathbb{Z}/m_1Z \times \mathbb{Z}/m_2Z$.

- If we have reduction type $[I_{m_1-m_2-m_3}]$, then we get

$$\#\Phi_v = m_1m_2 + m_1m_3 + m_2m_3$$

  according to Section 3.6.3. See Example 6.3 below.

- Reduction types $[I_0 - \mathcal{K} - l]$, where $\mathcal{K}$ is a Kodaira type of an elliptic curve and $l \geq 0$, only require $M_v \leq 4$ if $l = 0$, see Lemma 3.59. But if $l > 0$, then Conjecture 3.66 suggests that M_v depends not only on $v(\Delta)$, but also on the residue characteristic of v. Hence we can again expect large M_v in some cases.

- The situation for reduction type $[I_{m_1} - \mathcal{K} - l]$ is a combination of reduction type $[I_{m_1-0-0}]$ and of reduction type $[I_0 - \mathcal{K} - l]$, see Section 3.6.1.

We could give several examples where the current `Magma` implementation takes an insufferable amount of time, but our algorithm is very quick, for each of the cases discussed above. Yet this is not very interesting, since it does not tell us how our algorithm compares to a version of the algorithm of Flynn, Smart and Stoll that uses v-adic arithmetic. Instead we only discuss one interesting example that will be continued in the next section.

Example 6.1. Consider the curve C given as the smooth projective model over $\mathbb{Q}$ of the equation

$$\begin{aligned} Y^2 &= 1306881X^6 + 18610236X^5 - 46135758X^4 - 1536521592X^3 \\ &\quad - 2095359287X^2 + 32447351356X + 89852477764. \end{aligned}$$

This curve was found by Colin Stahlke in a systematic search for curves of genus 2 with many rational points. He shows in [90] that $\#C(\mathbb{Q}) \geq 366$ and Stoll has found 8 more points in $C(\mathbb{Q})$, see [98]. The given model is not minimal at $v = 2$ and we have $v_2(\Delta(C)) = 56$. A (globally) minimal model C' for C is given by

$$\begin{aligned} Y^2 + (-2X^3 + 3X^2 - 3X)Y &= 1306880X^6 + 5384478X^5 - 29895936X^4 \\ &\quad - 149001723X^3 + 129430735X^2 \\ &\quad + 1009320565X + 887232025; \end{aligned}$$

we have $v_2(\Delta(C')) = 26$. It turns out that C' has reduction type $[I_{5-9-12}]$ at $v = 2$ and so ε_2 factors through Φ_2 on the Jacobian J' of C'. However, the discussion of Section 3.6.3 tells us that $\#\Phi_2 = 213$. One can show that for

$$P = [(3, -358592) - (-2, -166188)]$$

we actually have $M_2 = 213$. In order to compute $\mu_2(P)$ using the algorithm by Flynn, Smart and Stoll, we therefore need to compute $\kappa(426P)$ and this is non-trivial even using 2-adic arithmetic, because we need a lot of precision. On the other hand, it is quite easy (and requires much less precision) to use our algorithm to compute all possible values of ε_2 and μ_2 after a few straightforward transformations without the need to compute any multiples and from this list all values of μ_2 can be read off. We will come back to this curve in Example 6.3 below.

Our algorithm is usually quite efficient, but sometimes it can become slow. So far we have only discussed the five different situations for which we have formulas for μ_v. In general the reduction of C may have a singularity of multiplicity at least 4 and then we need to apply the simplification procedure introduced in Proposition 3.36. In this case we do not get bounds on M_v in a simple way. Moreover, it can happen that the points on C mapping to the same singular point on the reduction are very close v-adically and so we need several iterations of the reduction procedure. Although this is done v-adically, we may have to work over large ramified field extensions. Hence it is possible that in these cases an optimized implementation of the algorithm due to Flynn and Smart using Stoll's refinements would actually be faster. However, we have found that in practice it is very rare that we need more than one iteration in the simplification process.

We do not discuss the archimedean contribution, because it turns out that without new tricks to compute theta functions, the method for computing μ_v when v is archimedean that was already introduced by Flynn and Smart is still the fastest available.

6.1.2 Improving the bound on the height constant

In Chapter 3 we have mentioned several possible improvements of bounds on the non-archimedean local height constant

$$\beta_v = \sup\{\mu_v(P) : P \in J(k_v)\}.$$

Recall that good bounds on the height constant are necessary if we want to compute generators of the Mordell-Weil group of J using the method given by Stoll in [94, §7], see Section 1.7. We will not repeat the improvements discussed in Chapter 3. Furthermore, we will not actually compute such generators, since that is not the topic of this thesis. Instead we give two

p	$v_p(2^4\mathrm{Disc}(F))$	bound on β_p	redn. type	new bound
2	20	16/3	$[I_{0-0-0}]$	2
3	6	4/3	$[II-III-0]$	4/3
5	26	17/3	$[I_0-II-1]$	4
305175781	6	2	$[I_{2-2-2}]$	1

Table 6.1: Bounds on local height constants for C_1

examples with large coefficients which show that our refinements can drastically reduce the previous bound on the height constant in some situations.

We will compare our bounds for the height constant to those obtained from Stoll's Proposition 3.11 and the improved bounds that can be computed using [92, §7].

Example 6.2. Let C_1 be given as the smooth projective model of

$$Y^2 = X^6 + 1220703126X^3 + 1220703125 = (X^3+1)(X^3+5^{13}).$$

The primes dividing the discriminant are $2, 3, 5$ and $305175781 = \frac{5^{13}-1}{4}$. Our strategy is to analyze the different reduction types of C. Note that this does not require the actual computation of a regular model, since the information we need drops out of our canonical height algorithm for free, except for the primes $p = 2$ and $p = 3$. But for $p = 2$ the given model is not minimal. Computing a 2-minimal model yields a regular model C_1'. Hence μ_2 vanishes on the Jacobian J_1' of C_1' and since the determinant of the transformation $\tau : C_1' \longrightarrow C_1$ has valuation equal to 2, we find that $\beta_2 = 2$.

For $p = 3$ there are two singularities of multiplicity 3 and hence we do not get a simple improvement of the bound. For $p = 5$, we have reduction type $[I_0-II-2]$, which means that β_5 can be bounded by $4 = 2\cdot 2$ according to Remark 3.69. Finally, we consider the prime $p = 305175781$. Here the reduction type is $[I_{2-2-2}]$; using our algorithm we find that the largest value that μ_p takes is 1.

Our findings are summarized in Table 6.1. The second column lists the bound that we get when we apply Proposition 3.11 and the third column contains the bound on β_p obtained as $B/3$, where B is the improved bound on

$$\gamma_p = \sup\{\varepsilon_p(P) : P \in J(k_p)\},$$

computed using the techniques of [92, §7]. The fourth column contains the reduction type of a p-minimal model of C_1; for $p \neq 2$ we can simply use C_1 and for $p = 2$ we take C_1'. In the last column we give the bound which we get using our knowledge of the reduction type.

Comparing the explicit global bounds, we find that Proposition 3.11 yields

$$65.890122 = 58.485758 + 7.404364,$$

p	$v_p(2^4\mathrm{Disc}(F))$	bound on β_p	redn. type	new bound
2	52	16	$[I_{5-9-12}]$	$\frac{1753}{213}$
3	13	11/3	$[III_9]$	11/3
5	11	11/3	$[I_{5-3-3}]$	2
7	4	2/3	$[I_0 - IV - 0]$	2/3
11	8	8/3	$[I_{2-3-3}]$	4/3
13	6	2	$[I_{2-2-2}]$	1
19	4	4/3	$[I_{1-1-2}]$	3/5
29	4	4/3	$[I_{1-1-2}]$	3/5
37	3	1	$[I_{1-1-1}]$	1/3

Table 6.2: Bounds on local height constants for C

where the first summand is the non-archimedean contribution and the second summand is the archimedean contribution. The techniques of [92, §7] improve this to

$$60.329401 = 52.925037 + 7.404364.$$

Finally, the bound that we get using our observations equals

$$36.229625 = 28.825261 + 7.404364.$$

Although this is still too large for practical purposes, it shows that we can get a significant improvement in some cases.

Our second example is a continuation of Example 6.1.

Example 6.3. Let C be given by

$$\begin{aligned} Y^2 &= 1306881X^6 + 18610236X^5 - 46135758X^4 - 1536521592X^3 \\ &\quad - 2095359287X^2 + 32447351356X + 89852477764. \end{aligned}$$

We proceed as in the previous example. See Table 6.2 for the results. We have left out prime factors which only divide the discriminant once, because according to [94, §5] they do not contribute toward the height constant.

For $p = 2$ we already know that the given model is not 2-minimal and we have given a minimal model C' in Example 6.1. Hence we can compute a bound on β_2 on J' and then use Remark 3.51 to compute a bound on J. For the other primes of reduction type $[I_{m_1-m_2-m_3}]$ we simply list all possible values which μ_p can take using the ideas of Section 3.6.3. For the prime $p = 3$ we get no improvement using our methods and for $p = 7$ we know that the existence of some $P \in J(\mathbb{Q}_7)$ such that $\varepsilon_7(P) = 2$ will prove that 2/3 is in fact an upper bound; it is easy to find such a point. For the other primes we use the results of Section 3.6.3 to quickly list all possible values of μ_p.

To sum up, we get an improvement of 20.86614 on the previous bound

$$54.60157 = 44.50728 + 10.09429,$$

where the first summand on the right hand side is the non-archimedean contribution and the second is the archimedean contribution to the bound.

Remark 6.4. It seems strange that C has reduction type $[I_{m_1-m_2-m_3}]$ for so many primes. However, in fact many of the curves containing a large number of rational points of genus 2 that we have analyzed exhibit this behavior; namely, they have such a reduction type for the majority of primes of bad reduction. This is due to the fact that if C has reduction type $[I_{m_1-m_2-m_3}]$ at a prime p, then $f(x)$ is a square modulo p and hence every x-coordinate yields a point on the reduction $\tilde{C}$.

6.2 Intersection theory

In this section we provide a hyperelliptic example of a regulator that was computed using the algorithm outlined in Chapter 5 and a non-hyperelliptic example for which we compute all non-archimedean data. In the latter case, the computation of the archimedean local Néron symbol is straightforward once the algorithms developed by Deconinck et al. have been reimplemented (see the discussion in Remark 5.24). Moreover, we shall discuss, at least in the case of hyperelliptic curves, how the running time changes as we increase

(a) the genus of the curve;

(b) the size of the coefficients of the point.

6.2.1 Hyperelliptic curves

We use the `Magma`-implementation of our algorithm to compute the regulator of the Jacobian of a hyperelliptic genus 3 curve up to an integral square. We have chosen an example where the 2-Selmer group could be computed quite easily, because all elements of the 2-torsion subgroup are defined over $\mathbb{Q}$. See [93] for an implementation-oriented description of the 2-descent algorithm; as usual, we have used `Magma` for the descent computations.

Example 6.5. Let C be given by the smooth projective model of the equation

$$Y^2 = X(X-1)(X-2)(X-3)(X-6)(X-8)(X+8).$$

The curve C is a hyperelliptic curve of genus 3, defined over $\mathbb{Q}$. A quick search reveals the following rational non-Weierstrass points on C.

$$(-2, \pm 240), (4, \pm 48), (-6, \pm 1008)$$

Let J denote the Jacobian of C; obviously its entire 2-torsion subgroup is defined over $\mathbb{Q}$. In order to bound the Mordell-Weil rank of J we compute the

prime	# of comps.	Φ_p	time
2	14	$(\mathbb{Z}/2\mathbb{Z})^5$	1.95s
3	9	$(\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/4\mathbb{Z}$	0.35s
5	4	$(\mathbb{Z}/2\mathbb{Z})^3$	0.23s
7	3	$(\mathbb{Z}/2\mathbb{Z})^2$	0.29s
11	2	$\mathbb{Z}/2\mathbb{Z}$	0.10s

Table 6.3: Regular model data

$S \in J(\mathbb{Q})$	$\hat{h}(S)$	time
P	1.900087075211040826920480902 66	23.10s
Q	1.152617936309056291065144470 88	19.76s
R	2.900908316163367270109402142 90	20.96s
$P+Q$	2.364815842037153818578368352 38	19.95s
$P+R$	5.515840785649853498445720299 52	20.67s
$Q+R$	5.749018934841371707555802193 03	21.22s

Table 6.4: Canonical height computations

dimension of the 2-Selmer group of J over $\mathbb{Q}$ using `Magma`. This dimension is equal to 3 and hence we get an upper bound of 3 on the rank.

We want to compute the regulator $\mathrm{Reg}(P, Q, R)$ of the subgroup G of $J(\mathbb{Q})$ generated by the points

$$\begin{aligned} P &= (-2, -240) - (\infty) \\ Q &= (4, -48) - (\infty) \\ R &= (-6, 1008) - (\infty). \end{aligned}$$

One can check using reduction modulo small good primes that these points are independent and hence that the rank is 3 and that G is a subgroup of finite index. Since $\mathrm{Reg}(P, Q, R)$ will turn out to be non-zero, we get another proof that G has finite index.

The discriminant of C factors as $2^{50}3^{12}5^6 7^4 11^2$. We first find regular models at the bad primes 2, 3, 5, 7 and 11. All computations in this example were done using `Magma` on a 1.73 GHz Pentium processor. It turns out that all computed regular models are already minimal; we list the number of components of the special fiber of the respective regular model, the (geometric) group of components Φ_p of the Néron model and the time it took to compute the regular model in Table 6.3.

After this preparatory step we now compute the entries of the height pairing matrix. The results and timings can be found in Table 6.4, Using these results, we find

$$\mathrm{Reg}(G) := \mathrm{Reg}(P, Q, R) = 4.288809861774632830588619343 66.$$

We can test our findings by computing $\mathrm{Reg}(nP, mQ, lR)$ for several integral values of n, m, l. In all cases we get the relation

$$\mathrm{Reg}(nP, mQ, lR)/\mathrm{Reg}(G) = n^2m^2l^2$$

up to an error of less than 10^{-27}, where the computations were done with real precision of 10^{30} and respective p-adic precisions of p^{100}.

Next we want to illustrate the behavior of the running time of our algorithm. We have refrained from a formal complexity analysis, mostly because the algorithm uses several external subroutines, such as the computation of regular models and of theta functions, whose complexities have not yet been analyzed. Moreover, a meaningful complexity analysis is made difficult by our usage of Gröbner bases whose complexity can be extremely problematic in general.

But in the case of zero-dimensional ideals of polynomial rings over fields, the complexity can be shown to be polynomial in D^n, where D is the maximal degree of the elements of the basis we start with and n is the number of variables. See [47] for a summary of results regarding complexity of Gröbner basis computations. In particular this holds for Faugère's $F4$-algorithm [38], used for instance by `Magma` (over fields and Euclidean rings). This result can be extended easily to the case of polynomial rings over Euclidean domains, provided we have fast algorithms available for the linear algebra computations in the $F4$-algorithm, such as those implemented in `Magma`. So the Gröbner basis computations do not cause any trouble in practice.

Indeed, the running time of the algorithm is usually dominated by the various analytic computations required for the archimedean local Néron symbols. They depend exponentially on the genus; the largest curve we have been able to compute with has genus 10, see Example 6.6 below. If the genus is not too large, but the size of the coefficients of the point $P \in J(k)$ that we want to compute the canonical height of is, then it turns out that the main bottlenecks are usually the factorizations alluded to in Section 5.3.2; recall that these are required in order to find out which places can lead to non-trivial non-archimedean local Néron symbols. See Example 6.7. The typical behavior is that the non-archimedean part of the computation is much faster than the archimedean part unless the former fails completely due to the factorisation problem.

All computations for the following two examples were done using a 3.00 GHz Xeon processor.

Example 6.6. Consider the family

$$C_d : y^2 = x^d + 3x^2 + 1$$

for $d \in \{5, 7, 9, 11, 13, 15, 17, 19, 21\}$ and let $P = [(0, 1) - (0, -1)] \in J_d(\mathbb{Q})$, where J_d is the Jacobian of C_d. We compute $\hat{h}(P)$ and record the running

d	genus	$\hat{h}(P)$	act	nact
5	2	1.209108948839430454915485486513	3.51s	0.33s
7	3	1.319353532098735151587742242 82	6.70s	0.34s
9	4	1.392372556781794225405948532 90	12.65s	0.87s
11	5	1.441873081167141031296676041 12	32.30s	1.67s
13	6	1.476796088419312452293964574 63	120.51s	2.99s
15	7	1.502657019791286715440057082 36	791.14s	5.17s
17	8	1.522540763524838385321488272 58	4729.03s	8.95s
19	9	1.538298826834028486665028188 88	62535.55s	14.20s
21	10	1.551091270847683786375492927 54	280731.59s	21.35s

Table 6.5: Canonical heights in a family

n	$\hat{h}(nP)$	act	nact
1	1.209108948839430454915485486513	3.00s	0.31s
2	4.836435795357721819661939460 57	3.15s	0.01s
3	10.881980539554874094239363 7862	2.93s	0.21s
4	19.345743181430887278647757842 1	3.28s	0.02s
5	30.227723720985761372887121628 1	3.11s	0.31s
6	43.527922158219496376957455144 7	3.29s	0.11s
7	59.246338493132092290858758391 5	3.47s	0.34s
8	77.382972725723549114591031368 5	3.90s	0.45s
9	97.937824855993866848154274075 2	4.31s	1.02s

Table 6.6: Canonical heights for multiples of a point

time for both the archimedean and the non-archimedean computations. See Table 6.5, where nact and act denote non-archimedean and archimedean computation time, respectively. This example hints at an exponential dependency on the genus.

Example 6.7. Next we look at the running times for positive multiples of $P \in J_5(\mathbb{Q})$. The results are in Table 6.6 and we see that we have $\hat{h}(nP) = n^2\hat{h}(P)$ for all $n \in \{1, \ldots, 9\}$. Here nact and act have the same meaning as in Table 6.5. We only get to $9P$, because for $10P$ the integer $q_{D,E,1}$ that has to be factored in order to find the possible primes of non-trivial intersection (see Section 5.3.2) is of order 10^{119} and must have at least two large prime factors; we have not succeeded in factoring it in nine days. But we see that our implementation performs reasonably well up to that point.

6.2.2 Non-hyperelliptic curves

Because our results from Chapter 5 are not limited to hyperelliptic curves, we would like to give an example of a regulator of (a subgroup of finite index of)

the Mordell-Weil group of a non-hyperelliptic Jacobian. The computation of the non-archimedean local Néron symbols can be done as in the hyperelliptic case, unless for some $v \in M_k^0$ we encounter k_v-rational divisors D and E whose supports are defined over local extension fields such that there is no single affine patch containing the entire intersection of the closures of D and E. In this case there are additional complications and we may have to restart our algorithm over an extension field of k. We refer to Section 5.3.4 for a discussion of this problem.

However, if $k = \mathbb{Q}$ and our divisors are supported in $\mathbb{Q}$-rational points to start with, then this difficulty cannot occur. Many interesting examples are of this form, because in practice one is often lead to regulators of Jacobians of curves that contain $\mathbb{Q}$-rational points. For such examples we can use our algorithm to compute the non-archimedean local Néron symbols.

The archimedean local Néron symbols are a different matter. See Remark 5.24 for a discussion of the current situation of the necessary algorithms described in Section 5.3.6. The best we can do is to give a list of explicit computations that yield the desired result once a suitable implementation exists. By virtue of Corollary 5.22 it suffices to list suitable divisors $D_{1,i}, D_{2,i}, E_{1,i}, E_{2,i}$ for $i = 1, \ldots, N$, where $N \geq 1$ is finite, such that computing the local Néron symbols $\langle D_{1,i} - D_{2,i}, E_{1,i} - E_{2,i} \rangle$ suffices. Here all $D_{1,i}$ and $D_{2,i}$ should be non-special with disjoint support and all $E_{1,i}$ and $E_{2,i}$ should have degree at most g.

Example 6.8. An example of a curve for which the computation of the regulator is interesting and useful is the curve $X_0^{\mathrm{dyn}}(6)$ considered by Stoll in [97]. It is a quotient of the curve $X_1^{\mathrm{dyn}}(6)$ which is a smooth projective curve that has an affine patch $Y_1^{\mathrm{dyn}}(6)$ parametrizing 6-cycles, that is pairs (x, c), where x is periodic of exact order 6 under the iteration

$$x_0 = x, \quad x_{n+1} = x_n^2 + c \quad \text{for } n \geq 0. \tag{6.1}$$

It is an interesting problem in arithmetic dynamics to determine whether there are rational N-cycles for a given N. The situation for $N = 2, 3, 4, 5$ is known and it is expected that there are no rational N-cycles for $N > 3$. See the introduction to [97]. Stoll shows, assuming the existence of an analytic continuation and functional equation of the L-series of J and the Birch and Swinnerton-Dyer conjecture for J that there are no rational 6-cycles, that is $x, c \in \mathbb{Q}$ satisfying (6.1). Here J is the Jacobian of $X_0^{\mathrm{dyn}}(6)$.

In order to give further evidence for this conditional statement, it would be helpful to verify the second part of the Birch and Swinnerton-Dyer conjecture 1.43 for $X_0^{\mathrm{dyn}}(6)$. Stoll has already computed several terms appearing in that statement and according to [97] it remains to show that

$$\mathrm{Reg}(J/\mathbb{Q})\Omega_J \#Ш(J/\mathbb{Q}) = 0.03483\ldots. \tag{6.2}$$

Recall that $\mathrm{Reg}(J/\mathbb{Q})$ is the regulator, Ω_J is the real period of the Néron differential and $Ш(J/\mathbb{Q})$ is the Shafarevich-Tate group of $J/\mathbb{Q}$. These terms are defined in [49, §F.4.1].

It can be shown that if $Ш(J/\mathbb{Q})$ is finite, then in this particular case its order must be a square. The real period Ω_J is probably not too hard to compute; for Jacobian surfaces a method due to Wetherell is reproduced in [44, §3.5]. So in order to check (6.2) up to an integral square, the main problem is the computation of the regulator of a subgroup of $J(\mathbb{Q})$ of finite index.

The curve $X_0^{\mathrm{dyn}}(6)$ is a non-hyperelliptic curve of genus 4 without any special properties. We refer to [97] for the construction of a model C of $X_0^{\mathrm{dyn}}(6)$ that is given by a curve of bidegree $(3,3)$ in $\mathbb{P}^1 \times \mathbb{P}^1$ with affine equation

$$G(u,w) = w^2(2+1)u^3 - (5w^2+w+1)u^2 - w(w^2-2w-7)u + (w+1)(w+3).$$

We will also use the image of this under the Segre embedding into $\mathbb{P}^3$. This yields a model C' of $X_0^{\mathrm{dyn}}(6)$ given by

$$\begin{aligned} &x_{10}x_{01} + x_{00}x_{11} = 0, \\ &x_{00}^3 - x_{00}x_{10}^2 + x_{00}^2x_{01} - 5x_{00}x_{10}x_{01} + 2x_{10}^2x_{01} - x_{10}x_{01}^2 + x_{10}^2x_{11} \\ &\quad + 7x_{10}x_{01}x_{11} - x_{01}^2x_{11} - 2x_{10}x_{11}^2 - 3x_{11}^3 = 0. \end{aligned}$$

In order to compute intersection numbers, we need to find a regular model over each $\mathrm{Spec}(\mathbb{Z}_p)$. Stoll has already computed such models. The only primes of singular reduction are $p = 2$ and $p = 8029187$; the reduction of C modulo the latter is regular, so only the prime $p = 2$ remains to be considered. Here Stoll finds a desingularization in the strong sense of the closure of C over $\mathrm{Spec}(\mathbb{Z}_2)$ consisting of two elliptic curves A and B and three rational curves S, S' and T. The corresponding intersection matrix is given by:

	A	B	S	S'	T
A	-4	2	1	1	0
B	2	-2	0	0	0
S	1	0	-2	0	1
S'	1	0	0	-2	1
T	0	0	1	1	-2

In [97, §3] Stoll lists ten rational points $P_0, \ldots, P_9 \in C(\mathbb{Q})$ (none of which come from a rational 6-cycle) and shows that the divisors supported in them generate a subgroup G of $J(\mathbb{Q})$ of rank 3. Moreover, he proves that the first part of the Birch and Swinnerton-Dyer conjecture predicts that the rank of $J(\mathbb{Q})$ is exactly 3, which would imply that G has finite index in $J(\mathbb{Q})$. We have listed coordinates for $P_0, \ldots, P_9$ on C and on C' in Table 6.7; here

	$((U_1 : U_2), (W_1 : W_2)) \in C$	$(x_{00} : x_{01} : x_{10} : x_{11}) \in C'$	cpt
P_0	$((0:1),(1:0))$	$(0:1:0:0)$	A
P_1	$((0:1),(-1:1))$	$(0:-1:0:1)$	B
P_2	$((0:1),(3:1))$	$(0:3:0:1)$	B
P_3	$((1:0),(0:1))$	$(0:0:1:0)$	A
P_4	$((1:1),(2:1))$	$(2:2:1:1)$	T
P_5	$((2:1),(1:1))$	$(2:1:2:1)$	B
P_6	$((1:1),(1:0))$	$(1:1:0:0)$	A
P_7	$((1:0),(-1:1))$	$(-1:0:1:0)$	A
P_8	$((-1:1),(1:0))$	$(-1:1:0:0)$	A
P_9	$((-4:5),(-1:1))$	$(4:-5:-4:5)$	B

Table 6.7: Rational points on models of $X_0^{\mathrm{dyn}}(6)$

$(U_1 : U_2)$ and $(W_1 : W_2)$ are the homogenizations of u and w, respectively, and cpt is the component on the regular model of C over $\mathrm{Spec}(\mathbb{Z}_2)$ given above that the respective point maps to. This component can be determined easily by following through the blow-ups necessary for the construction of the regular model.

Lemma 6.9. *Let $D = (P_0) - (P_1)$, let $E = (P_2) - (P_1)$ and let $F = (P_4) - (P_2)$. Then the points P, Q and R generate G, where*

$$P = [D],\ Q = [E] \text{ and } R = [F].$$

Moreover, we have

$$\begin{aligned} D &\sim (P_7) + (P_9) - (P_6) - (P_8) =: D' \\ E &\sim (P_3) + (P_5) + (P_6) - (P_0) - (P_7) - (P_9) =: E' \\ 2F &\sim (P_3) + 2(P_5) - (P_0) - 2(P_6) := F' \end{aligned}$$

Proof. This follows easily from the six independent linear equivalence relations between the (P_i) and subsequent remarks given in the proof of [97, Lemma 4]. □

For the next step, we need to compute the intersection multiplicities between different (P_i). It turns out that there are very few non-trivial intersections. Indeed we have (with the obvious abuse of notation)

$$i_2((P_6),(P_8)) = 1,\ i_2((P_1),(P_9)) = 1,\ i_5((P_7),(P_9)) = 1,$$

and all other intersection multiplicities are trivial. For $p \neq 2$ we can show this using Lemma 5.17. We also have that P_5 reduces to the same singular

point as P_1 and P_9 modulo 2, but blowing up this point separates the image of P_5 from the image of P_1 and P_9.

Using Lemma 6.9 we can now split up the computation of the terms appearing in the regulator of G as follows:

$$\begin{aligned}
\hat{h}(P) &= -\langle D, D\rangle = -\langle D, D'\rangle = -\sum_{p\in M_{\mathbb{Q}}^0} \langle D, D'\rangle_p - \langle D, D'\rangle_\infty \\
\hat{h}(Q) &= -\langle E, E\rangle = -\langle E, E'\rangle = -\sum_{p\in M_{\mathbb{Q}}^0} \langle E, E'\rangle_p - \langle E, E'\rangle_\infty \\
\hat{h}(R) &= -\langle F, F\rangle = -\frac{1}{2}\langle F, F'\rangle = -\sum_{p\in M_{\mathbb{Q}}^0} \frac{1}{2}\langle F, F'\rangle_p - \frac{1}{2}\langle F, F'\rangle_\infty \\
(P, Q) &= -\langle D, E\rangle = -\langle D', E\rangle = -\sum_{p\in M_{\mathbb{Q}}^0} \langle D', E\rangle_p - \langle D', E\rangle_\infty \\
(P, R) &= -\langle D, F\rangle = -\langle D, F\rangle = -\sum_{p\in M_{\mathbb{Q}}^0} \langle D, F\rangle_p - \langle D, F\rangle_\infty \\
(Q, R) &= -\langle E, F\rangle = -\langle E', F\rangle = -\sum_{p\in M_{\mathbb{Q}}^0} \langle E', F\rangle_p - \langle E', F\rangle_\infty
\end{aligned}$$

The correction terms at $p = 2$ are easily computed using one of the two approaches in Section 5.3.5, because we have the intersection matrix available and we know which components the P_i map to. This finishes the computation of the non-archimedean local Néron symbols.

Recall that for the computation of the archimedean local Néron symbol one of the divisors should be the difference of two non-special divisors with disjoint support. In the present situation this can be arranged easily. Combining everything, we have:

$$\begin{aligned}
\hat{h}(P) &= \frac{1}{2}\log 2 - \frac{1}{2}\langle D, 2D'\rangle_\infty \\
\hat{h}(Q) &= \log 2 - \frac{1}{4}\langle 4E, E'\rangle_\infty \\
\hat{h}(R) &= -\frac{1}{2}\log 2 - \frac{1}{8}\langle 4F, F'\rangle_\infty \\
(P, Q) &= -\log 2 - \frac{1}{2}\langle 2D', E\rangle_\infty \\
(P, R) &= \frac{1}{2}\log 2 - \frac{1}{4}\langle D, 4F\rangle_\infty \\
(Q, R) &= -\frac{1}{4}\langle E', 4F\rangle_\infty
\end{aligned}$$

For the computation of the archimedean local Néron symbols see Section 5.3.6 and the introduction to the present section. Since the algorithms of Deconinck et al. use Puiseux expansions, we are likely to need a plane curve

in $\mathbb{P}^2$ or $\mathbb{A}^2$ to construct the Riemann surface of the curve and this was the case in the Maple package. Since the algorithms are supposed to work on singular Riemann surfaces, this is not an essential restriction, since we can use a map to a suitable curve in $\mathbb{P}^2$ that is birationally equivalent to C'. This way it will be possible to complete the example once a new implementation of the necessary algorithms exists.

Appendix A

Proofs of some results from Chapter 3

A.1 Proof of Lemma 3.16

In this section we prove Lemma 3.16 using case distinctions and elementary algebraic manipulations. It would be interesting to find a more conceptual proof. In all cases F is of the form $F(X,Z) = f_1XZ^5 + f_3X^3Z^3 + f_5X^5Z$.

Case (a): $H = Z^3$, $f_5 \neq 0$

The identity $\widetilde{\delta_i}(x) = \widetilde{K}(x) = 0$ implies

$$0 = \widetilde{\delta_2}(x) + f_3\widetilde{K}(x) = f_5x_1^4$$

and thus $x_1 = 0$. We find $0 = \widetilde{\delta_1}(x) = f_5x_2^4$ and hence $x_2 = 0$. Then we also obtain $x_3 = 0$ from $0 = \widetilde{K}(x) = f_5x_3^4$ and thus $0 = \widetilde{\delta_4}(x) = x_4^4$ means that indeed $x_i = 0$ holds for all $i \in \{1,2,3,4\}$.

Case (b): $H = XZ^2$, $f_1f_5 \neq 0$

Similar to case (a) we have

$$0 = \widetilde{\delta_2}(x) + \widetilde{\delta_3}(x)\widetilde{K}(x) = f_5x_1^2x_3^2,$$

so we must have $x_1 = 0$ or $x_3 = 0$.

If $x_1 = 0$, then $0 = \delta_3(x) = f_5x_3^4$, thus x_3 vanishes. The Kummer surface equation then reads $0 = K(x) = x_2^2x_4^2$, whence $x_2 = 0$ or $x_4 = 0$ follow. However, if $x_2 = 0$, then we get $0 = \delta_4(x) = x_4^4$ and if $x_4 = 0$,

then we get $0 = \delta_4(x) = f_1^2 f_5^2 x_2^4$. Therefore we can deduce $x_i = 0$ for all $i \in \{1, 2, 3, 4\}$ in both subcases.

In the other case $x_3 = 0$ implies $0 = \delta_3(x) = f_1^2 x_1^4$, so x_1 vanishes and we are again in the situation already considered above.

Case (c): $H = X^2Z + XZ^2,\ f_1 f_5 (f_1 + f_3 + f_5 + f_1^2 + f_3^2 + f_5^2) \neq 0$

For this case, which is slightly more complicated than the two previous cases, we employ a case distinction on x_1. First we assume $x_1 = 0$ and show that necessarily the other x_i must be equal to zero as well. Then we suppose $x_1 \neq 0$ and derive a contradiction. We set $\beta := f_1 + f_3 + f_5 + f_1^2 + f_3^2 + f_5^2$.

So let $x_1 = 0$. Then we get

$$0 = \delta_3(x) = x_3^2(x_4 + f_5 x_3)$$

which means that we must have $x_3 = 0$ or $x_4 = f_5 x_3$.

If $x_3 = 0$, then $0 = K(x) = x_2^2 x_4^2$ implies $x_2 = 0$ or $x_4 = 0$. But from

$$0 = \delta_4(x) = x_4^4 + f_1^2 f_5^2 x_2^4$$

the result follows.

If we have $x_4 = f_5 x_3 \neq 0$ instead, then we find

$$0 = K(x) = f_5^2 x_3^2 (x_2 + x_3),$$

so that we get $x_2 = x_3 \neq 0$ and hence

$$0 = \delta_4(x) = f_5^2 \beta x_3^4,$$

a contradiction. This means that $x_1 = 0 = \delta_i(x)$ is only possible if we have $x_i = 0$ for all i.

Now we consider the case $x_1 \neq 0$, so we may assume that $x_1 = 1$. Here we get

$$0 = \delta_2(x) + f_3 K(x) = (1 + x_2 + x_3) x_3 (x_4 + f_1 + f_5 x_3).$$

If $x_3 = 0$, then we find

$$0 = \delta_1(x) = f_1^2 + x_4^2$$

which implies $x_4 = f_1$ and hence

$$K(x) = f_1^2 (1 + x_2)^2$$

from which the contradiction

$$0 = \delta_4(x) = f_1^2 \beta \tag{A.1}$$

follows.

Next we suppose that $x_4 = f_1 + f_5 x_3$, leading to $0 = \delta_1(x) = f_5^2 x_3^2 (1 + x_2 + x_3)^2$, so that either $x_3 = 0$ which leads to a contradiction by (A.1) or $1+x_2+x_3 = 0$ must hold. However, in that case we deduce $0 = K(x) = x_3^2 \beta$, so we get a contradiction anyway.

Finally, we assume that $1 + x_2 + x_3 = 0$ and obtain

$$0 = \delta_1(x) = (x_4 + f_1 + f_5 x_3)^2,$$

so we are in the case $x_4 + f_1 + f_5 x_3 = 0$ anyway, proving the lemma.

A.2 Proof of Lemma 3.18

In all cases our method is to first assume $x_1 = 0$ and then show that either $x_i = 0$ for all i or $y_i = 0$ for all i follows. To finish the claim, we assume $x_1 \neq 0$, so without loss of generality $x_1 = 1$, and then show that all y_i must be zero. We abbreviate $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$. There are a lot of nested case distinctions, so in order to follow the proof, the main difficulty is to remember at each step which assumptions were made. As in the case of Lemma 3.16 a conceptual proof would be of interest.

Case (a): $H = Z^3$

First we assume $x_1 = 0$. Then we get

$$0 = B_{12}(x, y) = f_5 x_2^2 y_1^2.$$

If $x_2 = 0$, but $y_1 \neq 0$, then we find

$$\begin{aligned} 0 &= B_{14}(x, y) = f_5 x_3^2 y_1^2, \\ 0 &= B_{11}(x, y) = x_4^2 y_1^2, \end{aligned}$$

so all x_i vanish.

If we have $y_1 = 0 \neq x_2$ instead, then all y_i are zero, because one can show that

$$\begin{aligned} 0 &= B_{14}(x, y) = f_5^2 x_2^2 y_2^2, \\ 0 &= B_{22}(x, y) = x_2^2 y_4^2, \\ 0 &= B_{11}(x, y) = f_5^2 x_2^2 y_3^2. \end{aligned}$$

The third case we have to look at is the case $x_2 = y_1 = 0$. In this situation we get $0 = B_{22}(x, y) = x_4^2 y_2^2$, so $x_4 = 0$ or $y_2 = 0$. We also have $0 = K(x) = f_5^2 x_3^4$ and hence $x_3 = 0$. So we may assume $y_2 = 0 \neq x_4$ which implies

$$0 = B_{33}(x, y) = (y_3 x_4)^2 \text{ and } 0 = B_{44}(x, y) = (x_4 y_4)^2,$$

therefore we get $y_3 = y_4 = 0$.

Now that we have finished proving that $x_1 = 0$ implies the lemma in case (a), the remaining step is to deduce that all y_i must be equal to zero under the assumption $x_1 = 1$. This follows quickly from the observation

$$0 = B_{12}(x, y) = f_5(y_2 + x_2 y_1)^2,$$

since then we have $y_2 = x_2 y_1$, leading to

$$\begin{aligned} & 0 = B_{23}(x, y) = f_5(y_3 + x_3 y_1)^2, \text{ so } y_3 = x_3 y_1 \\ \text{and} \quad & 0 = B_{11}(x, y) = (y_4 + x_4 y_1)^2, \text{ so } y_4 = x_4 y_1 \\ \text{and} \quad & 0 = B_{24}(x, y) = f_5^2 y_1^2. \end{aligned}$$

Hence all y_i vanish.

Case (b): $H = XZ^2$

Suppose $x_1 = 0$ and observe $0 = B_{12}(x, y) = f_5 x_3^2 y_1^2$, implying either $x_3 = 0$ or $y_1 = 0$.

If $x_3 = 0$, then we get

$$0 = K(x) = x_2^2 x_4^2, \text{ so } x_2 = 0 \text{ or } x_4 = 0.$$

If $x_2 = 0$, then we have

$$0 = B_{11}(x, y) = x_4^2 y_1^2 = B_{22}(x, y) = x_4^2 y_2^2 = B_{33}(x, y) = x_4^2 y_3^2$$

from which $x_i = 0$ for all i or $y_i = 0$ for all i follows.

If $x_4 = 0$, we observe that

$$\begin{aligned} 0 &= B_{11}(x, y) = f_5^2 x_2^2 y_3^2 = B_{22}(x, y) = x_2^2 y_4^2 = B_{33}(x, y) = f_1^2 x_2^2 y_1^2 \\ &= B_{44}(x, y) = f_1^2 f_5^2 x_2^2 y_2^2 \end{aligned}$$

and so we find again that $x_i = 0$ for all i or $y_i = 0$ for all i.

Now we suppose that $y_1 = 0 \neq x_3$. This has the following consequence:

$$0 = B_{34}(x, y) = f_5^2 x_3^2 y_3^2$$

Hence we get $y_3 = 0$, implying $0 = B_{33}(x, y) = x_3^2 y_4^2$ and $0 = B_{11}(x, y) = f_5^2 x_3^2 y_2^2$, therefore all y_i must vanish.

We now consider the case $x_1 = 1$. Then we obtain

$$0 = B_{34}(x, y) = y_1^2 (f_1 + f_5 x_3^2)^2 \tag{A.2}$$

and hence either $y_1 = 0$ or we can express f_1 as $f_1 = f_5 x_3^2$.

The first case is $y_1 = 0$, which implies $y_3 = 0$ and $0 = B_{23}(x, y) = x_3 y_2 y_4$.

If $x_3 = 0$, we get

$$0 = B_{11}(x, y) = y_4^2 \text{ and } 0 = B_{33}(x, y) = f_1^2 y_2^2,$$

thus $y_2 = y_4 = 0$.

If we have $y_2 = 0$ in (A.2), then again $0 = B_{11}(x, y) = y_4^2$, so $y_4 = 0$. Finally, if we have $y_4 = 0$ in (A.2), then $y_2 = 0$ follows from $0 = B_{33}(x, y) = f_1^2 y_2^2$.

In order to prove the lemma in case (b), it remains to prove it in the case $x_1 = 1, y_3 = x_3 y_1, f_1 = f_5 x_3^2$. Assuming this leads to $x_3 \neq 0$ and hence $y_3 = 0$. We also find

$$0 = B_{33}(x, y) = x_3^2(y_4 + x_4 y_1 + f_5 x_3(y_2 + y_1 x_2))^2 = 0, \tag{A.3}$$

whence $y_4 = x_4 y_1 + f_5 x_3(y_2 + y_1 x_2)$.

Using this relation we find

$$0 = B_{23}(x, y) = f_5 x_3^2 (y_2 + x_2 y_1)^2$$

and hence $y_2 = x_2 y_1$, whereby $y_1 = y_2 = 0$ follow from

$$0 = B_{24}(x, y) = f_5 x_3^2 y_1^2.$$

We also have $y_3 = 0$ from (A.2) and $y_4 = 0$ because of (A.3), which proves part (b) of the lemma.

Case (c): $H = X^2 Z + X Z^2, f_1 f_5 (f_1 + f_3 + f_5 + f_1^2 + f_3^2 + f_5^2) \neq 0$

Let $\beta := f_1 + f_3 + f_5 + f_1^2 + f_3^2 + f_5^2$. This is the trickiest case of the lemma, although it is, like the other cases, completely elementary. Having said that, we again start off by assuming $x_1 = 0$, yielding the following Kummer surface equation

$$0 = K(x) = (f_5 x_3^2 + x_2 x_4)^2$$

from which we get $f_5 x_3^2 = x_2 x_4$. In turn this implies

$$0 = B_{13}(x, y) = x_3 y_1 y_3 (x_4 + f_5 x_2).$$

Hence we have

$$x_3 = 0 \text{ or } y_1 = 0 \text{ or } y_3 = 0 \text{ or } x_4 = f_5 x_2. \tag{A.4}$$

We first assume $y_1 = 0$ and get

$$0 = B_{34}(x, y) = x_4 y_3 (y_4 + f_5 y_3)(x_2 + x_3)$$

and therefore

$$x_4 = 0 \text{ or } y_3 = 0 \text{ or } y_4 = f_5 y_3 \text{ or } x_2 = x_3. \tag{A.5}$$

We actually go through all the cases in (A.5). This is a rather tedious task, but we will be rewarded later on, as we can reuse several of the results in the other cases appearing in (A.4).

Suppose $y_3 = 0$. Then we get

$$0 = B_{33}(x, y) = x_3^2 y_4^2. \tag{A.6}$$

If $x_3 = 0$, then we have

$$0 = K(x) = x_2^2 x_4^2.$$

Now we find

$$x_2 = 0 \Rightarrow 0 = B_{22}(x, y) = x_4^2 y_2^2, 0 = B_{44}(x, y) = x_4^2 y_4^2$$

and

$$x_4 = 0 \Rightarrow 0 = B_{22}(x, y) = x_2^2 y_4^2, 0 = B_{44}(x, y) = f_1^2 f_5^2 x_2^2 y_2^2,$$

so we see that in both cases we either have $x_i = 0$ for all i or $y_i = 0$ for all i.

If $y_4 = 0$ holds in (A.6), then we get

$$0 = B_{22}(x, y) = x_4^2 y_2^2, \quad 0 = B_{44}(x, y) = f_1^2 f_5^2 x_2^2 y_2^2$$

so either $y_2 = 0$ or $x_2 = x_4 = 0$, in which case we have $0 = K(x) = f_5^2 x_3^4$. This finishes the case $y_3 = 0$ in (A.5).

If $x_4 = 0$ in (A.5), then we obtain

$$0 = B_{22}(x, y) = x_2^2 y_4^2, \quad 0 = B_{33}(x, y) = x_3^2 y_4^2,$$

so $y_4 = 0$ or $x_2 = x_3 = 0$.

If we have $x_2 = x_3 = 0$, this means that we are already done. If instead we have $y_4 = 0$, we get

$$0 = B_{11}(x, y) = f_5^2 x_2^2 y_3^2$$

We have already dealt with the case $y_3 = 0$, so we can assume $x_2 = 0$. But this leads to $0 = K(x) = f_5^2 x_3^4$ again.

The next case in (A.5) that we consider is the case $y_4 = f_5 y_3$ which implies $K(y) = f_5^2 y_3^2 (y_2 + y_3)^2$. Since we know that $y_3 = 0$ implies our claim, we can assume $y_2 = y_3 \neq 0$. Then we get

$$\begin{aligned} 0 &= B_{33}(x, y) = y_3^2 (x_4 + f_5 x_3)^2 \text{ and} \\ 0 &= B_{22}(x, y) = f_5^2 y_3^2 (x_2 + x_3)^2; \end{aligned}$$

therefore $x_4 = f_5 x_3$ and $x_2 = x_3$ follow, implying

$$0 = B_{44}(x, y) = f_5^2 \beta x_3^2 y_3^2,$$

and finally $x_2 = x_3 = 0$.

In order to finish off (A.5) we assume $x_2 = x_3$, thus

$$K(x) = x_3^2(f_5x_3 + x_4)^2.$$

Assuming $x_3 = 0$, we deduce from $x_2 = x_3 = 0$ and

$$\begin{aligned} 0 &= B_{22}(x,y) = x_4^2y_2^2 \\ 0 &= B_{33}(x,y) = x_4^2y_3^2 \\ 0 &= B_{44}(x,y) = x_4^2y_4^2 \end{aligned}$$

that we have either $x_i = 0$ for all i or $y_i = 0$ for all i.

So we consider the case $x_4 = f_5x_3 \neq 0$ and find that

$$0 = B_{33}(x,y) = x_3^2(y_4 + f_5y_3)^2.$$

Hence we have

$$0 = B_{22}(x,y) = f_5^2x_3^2(y_2 + y_3)^2.$$

But if $y_2 = y_3$, then $0 = B_{44}(x,y) = f_5^2\beta x_3^2y_3^2$ and so $y_3 = 0$, a case we have dealt with already. Therefore we have proved the assertion of the lemma for the case $x_1 = y_1 = 0$.

Now we go back to (A.4) and assume that $x_3 = 0$. The Kummer surface equation then tells us that either $x_2 = 0$ or $x_4 = 0$. But we find that

$$\begin{aligned} x_2 = 0 \Rightarrow 0 &= B_{11}(x,y) = x_4^2y_1^2 = B_{22}(x,y) = x_4^2y_2^2 \\ &= B_{33}(x,y) = x_4^2y_3^2 = B_{44}(x,y) = x_4^2y_4^2 \end{aligned}$$

and

$$\begin{aligned} x_4 = 0 \Rightarrow 0 &= B_{11}(x,y) = f_5^2x_2^1y_3^2 = B_{22}(x,y) = x_2^2y_4^2 \\ &= B_{33}(x,y) = f_1^2x_2^2y_1^2 = B_{44}(x,y) = f_1^2f_5^2x_2^2y_2^2. \end{aligned}$$

Thus we get that in both cases either $x_i = 0$ for all i or $y_i = 0$ for all i.

The next possible case from (A.4) is $y_3 = 0$. Because of what we have shown already, we can assume $y_1x_3 \neq 0$. We find that

$$0 = B_{23}(x,y) = y_1x_3(x_2 + x_3)(f_1y_1 + y_4),$$

so that either $x_2 = x_3 \neq 0$ or $y_4 = f_1y_1 \neq 0$. In the former case we have $0 = B_{33}(x,y) = x_3^2(y_4 + f_1y_1)^2$, so we are in the latter case anyway.

Accordingly we suppose $y_4 = f_1y_1 \neq 0$ which means that

$$K(y) = f_1^2y_1^2(y_1 + y_2)^2.$$

Thus $y_2 = y_1 \neq 0$ and from $0 = B_{44}(x,y) = f_1^2y_1^2(x_4 + f_5x_2)^2$ we get $x_4 = f_5x_2$ which ultimately leads to

$$0 = B_{22}(x,y) = \beta x_3^2y_1^2,$$

a contradiction. This finishes case (c) of the lemma in the case $x_1 = 0$.

Now we assume $x_1 = 1$. It turns out that it is a good idea to further distinguish between the cases $y_3 = 0$ and $y_3 \neq 0$.

We start with the case $y_3 = 0$ which leads to

$$0 = B_{11}(x, y) = (y_4 + x_4 y_1 + f_5 x_3 y_2)^2 \tag{A.7}$$

and thus

$$0 = B_{12}(x, y) = f_5 x_3 (y_1 + y_2)^2 = 0 \tag{A.8}$$

so that we either get $x_3 = 0$ or $y_1 = y_2$.

The assumption $x_3 = 0$ yields

$$0 = B_{14}(x, y) = (f_1(y_1 + x_4))^2 \Rightarrow y_1 = 0 \text{ or } x_4 = y_1.$$

If $y_1 = 0$, then $0 = B_{33}(x, y) = f_1^2 y_1^2$, so we conclude $y_2 = y_1 = 0$ by assumption and also $y_4 = 0$ due to (A.7), thus all y_i vanish.

If, on the other hand, $x_4 = f_1$ and $y_1 \neq 0$, then we have

$$0 = B_{22}(x, y) = f_1^2 (y_2 + x_2 y_1)^2;$$

therefore we get $y_2 = x_2 y_1$ and

$$0 = B_{24}(x, y) = f_1^2 y_1^2 (x_2 + 1)^2$$

which implies $0 = B_{44}(x, y) = f_1^2 \beta y_1^2$, contradicting our assumptions.

At this point we return to the other possible case in (A.8), namely the case $y_1 = y_2$. It leads to

$$0 = B_{14}(x, y) = y_2^2 (x_4 + f_1 + f_5 x_3),$$

that is $y_2 = 0$ or $x_4 = f_1 + f_5 x_3$. But $y_1 = y_2$ and (A.7) already imply that in the former case all y_i vanish, whereas in the latter case we can assume $y_2 \neq 0$ and $1 + x_2 + x_3 = 0$ from

$$0 = B_{33}(x, y) = f_1^2 y_2^2 (1 + x_2 + x_3)^2 = 0.$$

The final step is then to look at $B_{44}(x, y)$, which is equal to $f_1^2 \beta y_2^2$ and thus gives the desired contradiction.

The only remaining case is $x_1 = 1 = y_3$. The first helpful observation is

$$0 = B_{11}(x, y) = y_4 + y_1 x_4 + f_5 x_2 + f_5 x_3 y_2,$$

hence we must have

$$y_4 = y_1 x_4 + f_5 x_2 + f_5 x_3 y_2. \tag{A.9}$$

Using this consequence we obtain

$$x_2 = 1 + x_3 (y_1 + y_2)$$

from

$$0 = B_{12}(x, y) = f_5(x_2 + 1 + x_3(y_1 + y_2))^2.$$

Thus we deduce

$$0 = B_{34}(x, y) = y_1 x_3(x_4 + f_5 x_3 + f_1 y_1 + f_1 y_2)^2, \tag{A.10}$$

that is $y_1 = 0$ or $x_3 = 0$ or $x_4 = f_5 x_3 + f_1 y_1 + f_1 y_2$. We handle these cases separately.

Let us first suppose $y_1 = 0$, in which case we have

$$0 = B_{14}(x, y) = f_5^2 x_3^2 (y_2 + 1)^2 \tag{A.11}$$

and thus $x_3 = 0$ or $y_2 = 1$.

In case $y_2 = 1$, we consider $K(y) = (y_4 + f_5)^2$, so $y_4 = f_5$ and moreover

$$0 = B_{33}(x, y) = (x_4 + f_1 + f_5 x_3)^2$$

implying $0 = B_{22}(x, y) = \beta$ which cannot happen by assumption.

But if $x_3 = 0$ and $y_2 \neq 1$, then we observe $0 = B_{33}(x, y) = (x_4 + f_1 y_2)^2$, hence $0 = B_{23}(x, y) = f_1(1 + y_2)^2$ gives us a contradiction.

We proceed by assuming that $x_3 = 0 \neq y_1$ in (A.10); here we observe $0 = B_{14}(x, y) = y_1^2(x_4 + f_1)^2$, whereby $x_4 = f_1$. We then have $0 = B_{33}(x, y) = f_1^2(1 + y_1 + y_2)^2$, so that we can deduce $y_1 + y_2 + 1 = 0$ and thus $0 = B_{22}(x, y) = \beta$, a contradiction.

The upshot of this is that in order to finish the proof of the lemma we can assume we are in the case $x_1 = 1 = y_3$, $x_3 y_1 \neq 0$ and $x_4 = f_5 x_3 + f_1 y_1 + f_1 y_2$ (see (A.10)). We can see immediately that we have

$$0 = B_{23}(x, y) = f_1(1 + y_1 + y_2)^2(1 + x_3 y_1)^2.$$

Upon noticing

$$1 + y_1 + y_2 = 0 \Rightarrow 0 = B_{24}(x, y) = \beta x_3 y_1$$

we may thus assume that $x_3 y_1 = 1$ and $y_1 + y_2 \neq 1$.

We have

$$0 = B_{14}(x, y) = (1 + y_1 + y_2)^2(f_5 x_3 + f_1 y_1)^2,$$

resulting in $f_5 x_3 = f_1 y_1$. This relation allows us to obtain

$$x_4 = f_1 y_2$$

from (A.10) and hence $y_4 = f_1 y_1 y_2$ from (A.9). We also have $f_5 = f_5 x_3 y_1 = f_1 y_1^2$. Now we make these substitutions in $K(y)$ and find that

$$0 = K(y) = y_1^2(f_1^2 y_2^4 + f_1 y_2^2 + f_3 + f_3^2)$$

so that $f_1^2 y_2^4 = f_1 y_2^2 + f_3 + f_3^2$. But if we plug this into $B_{24}(x, y)$ we see that

$$0 = B_{24}(x, y) = f_1(y_1 + y_2 + 1)^2,$$

contradicting the assumption $y_1 + y_2 + 1 \neq 0$.

This finally completes the proof of the lemma.

A.3 Proof of Proposition 3.28

Recall that we must have $x_i \neq 0$ and $y_j \neq 0$ for some i, j.

Case (i)

This is part of the proof of [94, Proposition 3.2].

Case (ii)

Part (1): We have $\delta_4(x) = x_4^4$ and

$$\delta_4(x) = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta(x) = 0.$$

Part (2): We have $B_{44} = x_4^2 y_4^2$. If we assume $x_4 = 0 \neq y_4$ and $B = 0$, then we find $B_{ii} = x_i y_4^2$ for $i = 1, 2, 3$, so

$$B = 0 \Rightarrow x_4 = y_4 = 0 \Rightarrow \delta(x) = \delta(y) = 0.$$

Case (iii)

Part (1): We have $\delta_4(x) = x_4^4$ and

$$\delta_4(x) = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta(x) = 0.$$

However,

$$x_4 = 0 \Rightarrow K(x) = a^2 x_1^4 \Rightarrow x_1 = 0.$$

Part (2): We have $B_{44} = x_4^2 y_4^2$. If we assume $x_4 = 0 \neq y_4$ and $B = 0$, then we find $B_{ii} = x_i y_4^2$ for $i = 1, 2, 3$, so

$$B = 0 \Rightarrow x_4 = y_4 = 0 \Rightarrow \delta(x) = \delta(y) = 0.$$

Case (iv)

Part (1): We have $\delta_1(x) = x_1^2 x_4^2,\ \delta_2(x) = 0,\ \delta_3(x) = a^2 x_1^4,\ \delta_4(x) = x_4^4$. But we also have

$$K(x) = x_2^2 x_4^2 + x_1^2 x_3 x_4 + a^2 x_1^4$$

and hence

$$\delta_4(x) = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta(x) = 0,$$

with the additional condition $x_1 = 0$.
Part (2): We have $B_{44} = x_4^2 y_4^2$. If we assume $x_4 = 0 \neq y_4$ and $B = 0$, then we find $B_{ii} = x_i y_4^2$ for $i = 1, 2, 3$, so

$$B = 0 \Rightarrow x_4 = y_4 = 0 \Rightarrow \delta(x) = \delta(y) = 0.$$

Case (v)

Part (1): We have $\delta_1(x) = 0,\ \delta_2(x) = a^2x_1^2x_3^2 = K(x),\ \delta_3(x) = 0, \delta_4(x) = x_4^4$, so

$$\delta_4(x) = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta(x) = 0,$$

with the additional condition $x_1x_3 = 0$.
Part (2): We have $B_{44} = x_4^2y_4^2$. If we assume $x_4 = 0 \neq y_4$ and $B = 0$, we get $B_{11} = x_1^2y_4^2$ and $B_{33} = x_3^2y_4^2$. Hence $x_1 = x_3 = 0$ which yields $B_{22} = x_2^2y_4^2$ and thus

$$B = 0 \Rightarrow x_4 = y_4 = 0 \Rightarrow \delta(x) = \delta(y) = 0.$$

Case (vi)

Part (1): We have $\delta_1(x) = b^2x_1^4$, so $\delta(x) = 0$ implies $x_1 = 0$, which in turn leads to $\delta_4(x) = x_4^4$. Since $x_1 = x_4 = 0$ implies $\delta(x) = 0$, we get

$$\delta_1(x) = \delta_4(x) = 0 \Leftrightarrow x_1 = x_4 = 0 \Leftrightarrow \delta(x) = 0.$$

Part (2): We have $B_{14} = b^2x_1^2y_1^2 = 0$. If we assume $B = 0$ and $x_1 = 0 \neq y_1$, we get $B_{11} = x_4^2y_1^2$, so $x_4 = 0$ and $B_{23} = b^2x_2^2y_1^2$ follow. From $x_2 = 0$ we deduce $B_{22} = b^2x_3^2y_1^2$, so we get the contradiction $x = 0$ and hence we have $x_1 = y_1 = 0$. But this means that we have

$$B_{44} = x_4^2y_4^2, B_{22} = x_4^2y_2^2 + x_2^2y_4^2, B_{33} = x_3^2y_4^2 + x_4^2y_3^2.$$

From this we get $x_4 = y_4 = 0$ and hence $\delta(x) = \delta(y) = 0$.

Case (vii)

The proof is the same as in case (ii).

Case (viii)

Part (1): We have $\delta_4(x) = x_4^4$ and in fact

$$\delta_4(x) = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta(x) = 0$$

as in case (ii).
Part (2): We have $B_{44} = x_4^2y_4^2$, but if we suppose $B = 0$ and $x_4 = 0 \neq y_4$, we find $B_{11} = x_1^2y_4^2$ and $B_{33} = x_3^2y_4^2$. Together these imply $x_1 = x_3 = 0$ and moreover $B_{22} = x_2^2y_4^2$, so we get $x = 0$, a contradiction. Thus we conclude

$$B = 0 \Rightarrow x_4 = y_4 = 0 \Rightarrow \delta(x) = \delta(y) = 0.$$

Case (ix)

Part (1): We have $\delta_4(x) = x_4^4$, so from $\delta(x) = 0$ it follows that $x_4 = 0$ and thus $\delta_1(x) = \delta_3(x) = 0$. Furthermore, we get

$$\delta_2(x) = b(b^2 + b)x_1^2 x_3^2 = bK(x),$$

so $\delta_4(x) = 0 \Leftrightarrow x_4 = 0$ with the additional condition $x_1 x_3 = 0$.
Part (2): The same proof given in case (viii), part (2), works here as well.

Case (x)

Part (1): We have $\delta_1(x) = x_1^2(x_4 + ax_1)^2$. If $x_1 = 0$, then $\delta_4(x) = x_4^4$ and since $x_1 = x_4 = 0$ implies $\delta(x) = 0$, this case is finished. If we assume $x_4 = ax_1 \neq 0$, however, then we find $\delta_4(x) = (a^2 + a + b + b^2)x_1^4$, so we cannot have $\delta(x) = 0$.
Part (2): This is the most tedious part of the proof. We distinguish between the cases $x_1 = 0$ and $x_1 \neq 0$ and start with the former. We find $B_{44} = x_4^2 y_4^2$ and suppose that we have both $B = 0$ and $x_4 = 0 \neq y_4$. Then we may assume $y_4 = 1$, so $B_{33} = (x_3 + ax_2 y_1)^2$ and therefore $x_3 = ax_2 y_1$. From this we can see that

$$B_{23} = ax_2^2 y_1^2(1 + ay_1^2),$$

i.e. $x_2 y_1(1 + ay_1) = 0$.

- If $x_2 = 0$, then also $x_3 = ax_2 y_1 = 0$, and we get the contradiction $x = 0$.
- If $y_1 = 0$, then $x_3 = ax_2 y_1 = 0$ and $B_{22} = x_2^2$, so again we have $x = 0$.
- If $ay_1 = 1$, then $x_3 = ax_2 y_1 = x_2$ and this implies

  $$B_{22} = x_2^2(1 + ay_1^2 + b^2 y_1^2 + by_1^2) = (a^2 + a + b + b^2)x_2^2 y_1^2,$$

  which is impossible, since we must be in one of the two cases already treated.

Therefore we find that $x_1 = x_4 = 0$ necessarily means that y_4 vanishes. But since we then have $B_{33} = a^2 x_2^2 y_1^2$, and the assumption $y_1 \neq 0$ implies $x_2 = 0$ and $B_{23} = ax_3^2 y_1^2$, hence $x = 0$, we deduce

$$B = x_1 = 0 \Rightarrow \delta(x) = \delta(y) = 0.$$

Next we consider the situation $B = 0, x_1 \neq 0$ and we want to derive a contradiction. We may assume $x_1 = 1$ and find $B_{11} = y_4^2 + x_4^2 y_1^2$, so $y_4 = x_4 y_1$, in turn implying $B_{1,4} = y_1^2(a + x_4)^2$. Hence we either have $y_1 = 0$ or $y_1 \neq 0, x_4 = a$.

- If $y_1 = 0$, then also $y_4 = 0$ and thus $B_{33} = (ay_2 + x_4y_3)^2 = 0$. But because of this we find

$$B_{23} = x_4^2y_3^2 + x_4y_2y_3 + ay_2y_3 + ay_3^2 = y_3^2(x_4 + a)^2$$

  which implies $x_4 = a$ and thus $y_2 = y_3$. The contradiction is now immediate from $B_{22} = (a^2 + a + b + b^2)y_3^2$.

- If $y_1 \neq 0$ and $x_4 = a$, we find $y_4 = ay_1$, whereby $B_{44} = a^2(a^2 + a + b + b^2)y_1^2$. But since by assumption none of the factors vanish, we end up with another contradiction, as desired.

Case (xi)

Part (1): We have $\delta_3(x) = a^2x_1^4$, so $x_1 = 0$ follows from $\delta(x) = 0$. But this implies $\delta_4(x) = x_4^4$ and $x_1 = x_4 = 0$ means that we have $\delta(x) = 0$, so

$$\delta_1(x) = \delta_4(x) = 0 \Leftrightarrow x_1 = x_4 = 0 \Leftrightarrow \delta(x) = 0.$$

Part (2): We have $B_{34} = a^2x_1^2y_1^2$, so $x_1y_1 = 0$ if $B = 0$. We assume $x_1 = 0 \neq y_1$ and find $B_{11} = x_4^2y_1^2$, implying $x_4 = 0$ and hence $B_{33} = x_3^2y_4^2 + a^2x_2^2y_1^2$, $B_{22} = x_2^2y_4^2 + b^2x_3^2y_1^2$ and $B_{23} = x_2x_3y_1y_4$.

- If $x_2 = 0$, then $B_{22} = b^2x_3^2y_1^2$.
- If $x_3 = 0$, then $B_{33} = x_2^2y_1^2$.
- If $y_4 = 0$, then $B_{22} = b^2x_3^2y_1^2, B_{33} = x_2^2y_1^2$.

Since these all lead to the contradiction $x = 0$, we must have $y_1 = 0$, but from this $x_4 = y_4 = 0$ and thus $\delta(x) = \delta(y) = 0$ follow exactly as in case (vi).

Case (xii)

This is part of the proof of [94, Proposition 3.2].

Case (xiii)

This is also part of the proof of [94, Proposition 3.2].

A.4 Proof of Lemma 3.46

Proof. (for $v(2) = 0$)

Let $i \in \{0, \ldots, m-1\}$. Since ε_v factors through the component group Φ, it suffices to find a single P satisfying $\chi(P) = i$ and $\varepsilon_v(P) = 2\min\{\chi(P), m - \chi(P)\}$ to show that the lemma holds for i.

If $i = 0$, then we can use $\varepsilon_v(O) = 0$, where O is the origin or more generally any point in the kernel of reduction.

Let $0 < i < m/2$. An unramified field extension yields an affine point P_1 on C such that $v(z(P_1)) = i$. Let P_2 be any affine point mapping to $B_0 = A$ such that $z(P_2) = 0$. Then the point $P = [(P_1) - (P_2)]$ on the Jacobian satisfies

$$\chi(P) \in \{i, m - i\}.$$

Here we may assume that $\chi(P) = i$, since we could take P_1^- instead of P_1 if need be, where P_1^- is the image of P_1 under the hyperelliptic involution.

Let $x = (x_1, x_2, x_3, x_4)$ be a set of Kummer coordinates for P such that $x_3 = 1$. Then we see that $n := v(x_1) = v(z(P_1))$, $v(x_2) = 0$ and $v(x_4) \geq n$ hold. We now take a closer look at the valuations of the entries of the quadruple $\delta(x) = (\delta_1(x), \delta_2(x), \delta_3(x), \delta_4(x))$. One can check easily that $v(\delta_i(x)) \geq 2n$ holds for all $i \in \{1 \ldots, 4\}$.

Now we distinguish cases. If $n < v(x_4)$, then the unique term of valuation equal to $2n$ appearing in $\delta_3(x)$ is

$$4f_1^2 f_4 x_1^2 x_2^2 \neq 0$$

and hence we get $\varepsilon_v(P) = v(\delta(x)) = 2n = 2\min\{\chi(P), m - \chi(P)\}$.

The case $v(x_4) = n$ is more difficult. Here we find that $v(\delta_2(x)) = 2n$ if the following expression has valuation equal to $2n$, because the valuations of all other summands are strictly larger than $2n$:

$$\begin{aligned} r \;=\; & 16x_1^2x_3^2(f_1f_4^2 - 20f_2f_3f_4 + 5f_3^3) + x_4^2(5x_2^2f_3 + 8x_2x_3f_4) + 2x_4(4x_1x_2^2 \\ & f_1f_4 + 8x_1x_2x_3f_2f_4 - 5x_1x_2x_3f_3^2 - 6x_1x_3^2f_3f_4) - 12x_1^2x_2x_3f_1f_3f_4 \end{aligned}$$

Next we assume that $v(r) > 2n$ and show that it puts severe restrictions on P_2.

We can use the fact that $x = (x_1, x_2, x_3, x_4)$ satisfies the defining equation $K(x) = 0$ of the Kummer surface, and the fact that since all summands of $\delta_3(x)$ have valuation greater than $2n$, except for possibly $4f_4(f_1x_1x_2 - x_3x_4)^2$, our assumption $v(r) > 2n$ leads to

$$f_1x_1x_2 - x_3x_4 \equiv 0 \pmod{\pi^{n+1}}.$$

Playing around with these two ingredients (and skipping the rather tiresome details), we arrive at the following necessary condition for r to satisfy $v(r) > 2n$:

$$4f_1f_4z(P_2)^2 - (8f_3f_4 - 5f_2f_3)z(P_2) + 4f_4^2 \equiv 0 \pmod{\pi} \tag{A.12}$$

However, there can be at most two possible values for the reduction of $z(P_2)$ satisfying (A.12), hence we can, after possibly making another unramified field extension, find a point on the reduction of the curve that does not

satisfy (A.12). We lift it to C and set P_2 equal to it to find a point on J that satisfies

$$\varepsilon_v(P) = v(\delta_3(x)) = 2n = 2\min\{\chi(P), m - \chi(P)\}.$$

The last remaining case is when m is even and $\chi(P) = m/2$. We pick $P = [(P_1) - (P_2)]$ with $v(z(P_1)) \geq m/2$ and $v(z(P_2)) = 0$. Then we get $v(\delta_i(x)) \geq m$ for $i \in \{1, 2, 3, 4\}$. However, Stoll proves in [94] that in general $v(\Delta)$ is an upper bound for $\varepsilon_v(P)$, so that

$$\varepsilon_v(P) = m = 2\chi(P) = 2\min\{\chi(P), m - \chi(P)\}$$

follows. The proof for $v(2) > 0$ is analogous. □

A.5 Proof of Lemma 3.47

Proof. (for $v(2) = 0$)

The lemma holds trivially in several cases, namely when either P_1 or P_2 map to A (use the proof Lemma 3.46), when $\chi(P) = m/2$ (dito) or when $\chi(P) = 0$ (as $\varepsilon_v(P) = 0 \Leftrightarrow v(x_1)v(x_4) = 0$).

So we can assume $0 < v(z(P_1))$, $0 < v(z(P_2))$, implying $v(x_2) > 0$ and $w(P) = \min\{v(x_1), v(x_4)\} < m/2$. We show that we have $\varepsilon_v(P) = 2w(P)$ directly; the first equality was the subject of Lemma 3.46. The two cases to be considered are

(a) $v(x_1) < v(x_4)$

(b) $v(x_4) \leq v(x_1)$.

In case (a) we find $\delta_i(x) \geq 2v(x_1)$ for all $i \in \{1, 2, 3, 4\}$. In particular the coefficient of $x_1^2 x_3^2$ in $\delta_2(x)$ is equal to

$$16 f_1 f_4^2 - 5 f_3 (4 f_2 f_4 - f_3^2)$$

and all other summands in $\delta_2(x)$ have valuation strictly larger than $2v(x_1)$. However, the Kummer surface equation $K(x) = 0$ satisfies

$$K(x) \equiv (f_3^2 - 4 f_2 f_4) x_1^2 x_3^2 \pmod{\pi^{2n+1}},$$

where $n = v(x_1)$. Therefore we get

$$\delta_2(x) \equiv 16 f_1 f_4^2 x_1^2 x_3^3 \pmod{\pi^{2n+1}}$$

and thus

$$v(\delta(x)) = 2v(x_1) = 2w(P).$$

In case (b) we have $\delta_i(x) \geq 2v(x_4)$ for all $i \in \{1, 2, 3, 4\}$ and $v(\delta_3(x)) = 2v(x_4)$; here the unique term in $\delta_3(x)$ with lowest valuation is $4 f_4 x_3^2 x_4^2$. Hence we deduce

$$v(\delta(x)) = 2v(x_4) = 2w(P).$$

□

A.6 Proof of Lemma 3.53

Proof. We assume that $v(2) = 0$. The proof for residue characteristic 2 is virtually the same. We first assume $v(x_1)v(x_3) = 0$. By symmetry we may assume $v(x_1) > 0$ and $v(x_3) = 0$; then we obviously have $\chi_2(P) = 0$. We start with the assumption $v(x_1) < m_1/2$. Then we get $v(x_1) < v(x_4)$, implying $K(x) \equiv (f_3^2 - 4f_2f_4)x_1^2x_3^2 \pmod{\pi^{2v(x_1)+1}}$ which is impossible, therefore

$$v(x_4) \leq v(x_1)$$

follows. Then we see that

$$v(\delta_2(x)) = v(f_4x_3^2x_4^2) = 2v(x_4),$$

and hence from inspection of the other $\delta_i(x)$ we deduce that $\varepsilon_v(P) = 2v(x_4)$.

If $v(x_2) = 0$, then we also have

$$v(x_1) < v(x_4),$$

leading to

$$K(x) \equiv x_2^2x_4^2 \pmod{\pi^{2v(x_4)+1}}.$$

Thus we get $v(x_1) = v(x_4)$ and hence

$$\varepsilon_v(P) = 2v(x_4) = 2v(x_1) = 2\min\{\chi_1(P), m_1 - \chi_1(P)\}.$$

But the fact that for any $0 \leq i < m_1/2$ we can find a point P_1 (possibly defined over an unramified extension of the base field) satisfying $v(z(P_1)) = i$ implies that we also have

$$\varepsilon_v(P) = 2\min\{\chi_1(P), m_1 - \chi_1(P)\} = 2v(x_4)$$

for those x that satisfy $v(x_2) > 0$

Now we look at the case when both x_1 and x_3 have positive valuation, whence $v(x_2) = 0$. If $v(x_1) < m_1/2$ and $v(x_3) < m_2/2$, then the definition of x_4 implies that we must have

$$v(x_4) \geq v(x_1) + v(x_3).$$

However, if $v(x_4)$ were strictly larger than $v(x_1)+v(x_3)$, then $K(x)$ would be congruent to $(f_3^2 - 4f_2f_4)x_1^2x_3^2$ modulo $\pi^{2v(x_1)+2v(x_3)+1}$, which is impossible, since $(f_3^2 - 4f_2f_4)$ does not vanish modulo π. Hence we deduce

$$v(x_4) = v(x_1) + v(x_3)$$

and in this case the Kummer surface equation yields

$$v((f_3^2 - 4f_2f_4)x_1^2x_3^2 + x_2^2x_4^2 - 2f_3x_1x_2x_3x_4) > 2(v(x_1) + v(x_3)). \quad \text{(A.13)}$$

It is easy to see that the $\delta_i(x)$ satisfy $v(\delta_i(x)) \geq 2(v(x_1) + v(x_3))$ for all i. A closer look at $\delta_2(x)$ reveals that the sum of the terms of lowest valuation in $\delta_2(x)$ is equal to

$$5f_3((f_3^2 - 4f_2f_4)x_1^2x_3^2 + x_2^2x_4^2 - 2f_3x_1x_2x_3x_4) + 16f_2f_2x_1x_2x_3x_4,$$

so that by (A.13) we have

$$v(\delta_2(x)) = v(16f_2f_2x_1x_2x_3x_4) = v(x_1) + v(x_3) + v(x_4) = 2(v(x_1) + v(x_3)).$$

The possible images of P under χ are listed below:

$$(v(x_1), v(x_3)), (m_1 - v(x_1), v(x_3))(v(x_1), m_2 - v(x_3)), (m_1 - v(x_1), m_2 - v(x_3))$$

Hence

$$\varepsilon_v(P) = 2(\min\{\chi_1(P), m_1 - \chi_1(P)\} + \min\{\chi_2(P), m_2 - \chi_2(P)\})$$

follows.

In all remaining cases we have $v(x_1) \geq m_1/2$ or $v(x_3) \geq m_2/2$ and by symmetry we may assume the latter. If we assume that $0 < v(x_4) < m_3/2 + 2v(x_1)$ holds, then we get

$$K(x) \equiv x_2^2x_4^2 \equiv 0 \pmod{\pi^{2v(x_4)+1}},$$

a contradiction. Hence we see that $v(x_4)$ is at least $m_3/2 + 2v(x_1)$ and it follows easily that $v(\delta_i(x)) \geq m_3 + 2v(x_1)$ holds.

First suppose $0 < v(x_1) < m_1/2$. In this case we find that

$$\delta_3(x) \equiv 4(f_1^2f_2 + 4f_0f_2f_4)x_1^2x_2^2 \pmod{\pi^{m_3+2v(x_1)+1}}$$

and therefore

$$\varepsilon_v(P) = v(\delta_3(x)) = m_3 + 2v(x_1) = 2\min\{\chi_1(P), m_1 - \chi_1(P)\} + 2\chi_2(P).$$

We proceed with the case $v(x_1) = 0$ and observe

$$\delta_4(x) \equiv (f_1^2 + 4f_0f_2)(f_3^2 - 4f_2f_4)x_1^4 \pmod{\pi^{m_3+1}},$$

whence

$$\varepsilon_v(P) = v(\delta_4(x)) = m_3 = 2\chi_2(P).$$

Finally, if $v(x_1) \geq m_1/2$ and $v(x_3) \geq m_2/2$, then all $\delta_i(x)$ satisfy $\delta_i(x) \geq m_1 + m_2$. By Stoll's bound from [92] this is also an upper bound for ε_v, so we get

$$\varepsilon_v(P) = m_1 + m_2 = 2\chi_1(P) + 2\chi_2(P).$$

This finally finishes the proof of Lemma 3.53. □

A.7 Proof of Proposition 3.56

Proof. Again we give the proof only when $v(2) = 0$, the complementary case being entirely analogous.

In order to obtain formulas for μ_v in this case, we first observe that in contrast to case (2) we have

$$f_3^2 - 4f_2f_4 \equiv 0 \pmod{\pi}$$

and moreover a closer look at the coefficients of the F_i tells us

$$v(f_3^2 - 4f_2f_4) \geq \min\{m_1, m_2, m_3\}.$$

We first consider points $P = [(P_1) - (P_2)]$ where $P_1, P_2 \in C(k_v)$ are nonsingular and map to distinct components of the special fiber, so without loss of generality P_1 maps to A and P_2 maps to E. In this case we obtain $v(x_4) > 0$ and the computation of $\varepsilon_v(P)$ goes as follows:

We first show that we must have

$$v(x_4) \geq \min\{m_1, m_2, m_3\}.$$

Supposing the contrary, the Kummer surface equation reduces to

$$K(x_1, x_2, x_3, x_4) \equiv -2x_1x_3x_4(2f_2x_1 + f_3x_2 + 2f_4x_3) \equiv 0 \pmod{\pi^{v(x_4+1)}})$$

and this cannot happen, because the term in parentheses reduces to

$$2(1 - x(\widetilde{P_1}))(1 - x(\widetilde{P_2}))$$

which is non-zero, since neither P_1 nor P_2 reduce to the singular point $(1, 0)$.

We also find that $m_1 = \min\{m_1, m_2, m_3\}$ implies $\varepsilon_v(P) = v(\delta_1(x)) = m_1$. By symmetry we also obtain $\varepsilon_v(P) = v(\delta_3(x)) = m_3$ whenever $m_3 = \min\{m_1, m_2, m_3\}$ and if the inequality $m_2 < \min\{m_1, m_3\}$ holds, then we have $\varepsilon_v(P) = v(\delta_2(x)) = m_2$.

Next we consider the cases $P \mapsto [D_i - A]$ and $P \mapsto [D_i - E]$. Clearly we may assume $i \leq m_3/2$ (otherwise use $-P$); in fact we first deal with the case $i < m_3/2$. We know that $v(x_3) = v(x(P_1)) = i$ and $v(x_1) = v(x_2) = 0$. Our usual observation tells us that we cannot have $v(x_4) < v(x_3)$, since that would imply

$$K(x_1, x_2, x_3, x_4) \equiv x_2^2x_4^2 \pmod{\pi^{2v(x_4)+1}}.$$

Let $x(P_1) = x'(P_1)\pi^i$ and $y(P_1) = y'(P_1)\pi^i$. Also let $x_4' := \pi^{-i}x_4(x(P_1) - x(P_2))^2$. Then we have

$$\begin{aligned} x_4' &\equiv 2f_2x'(P_1)x(P_2) + f_3x'(P_1)x(P_2)(x(P_1) + x(P_2)) + 2y'(P_1)y(P_2) \\ &\equiv 2x'(P_1)x(P_2)(1 - x(P_2)) + 2y'(P_1)y(P_2) \pmod{\pi}. \end{aligned}$$

Since $P_1 \mapsto D_i$ we have $y'(P_1) \equiv -x'(P_1) \pmod{\pi}$. If we now suppose that, in addition, we have $y(P_2) \equiv x(P_2)(x(P_2)-1) \pmod{\pi}$ (case $[D_i - A]$), then

$$x_4' \equiv 4x'(P_1)x(P_2)(1-x(P_2)) \not\equiv 0 \pmod{\pi} \tag{A.14}$$

and hence $v(x_4) = v(x_3) = i$ follow. Moreover, we have

$$\varepsilon_v(P) = v(\delta_1(x)) = 2v(x_4) = 2i.$$

Of course this result also gives us the values of ε_v on the components $[B_i - A]$ and $[C_i - A]$ in terms of i, where i satisfies $i < m_1/2$ and $i < m_2/2$, respectively.

The case $[D_i - E]$, i.e $y(P_2) \equiv -x(P_2)(x(P_2)-1) \pmod{\pi}$, is more difficult, since then $v(x_4) > v(x_3) = i$ holds (see (A.14)) and we need to look more closely at the duplication polynomials.

Recall that we have set

$$m_4 = \min\{v(x_3) + v(f_3^2 - 4f_2f_4), v(x_3) + v(f_5), v(x_3) + v(f_6), m_3 - v(x_3)\}.$$

Lemma A.1. *If P maps to $[D_i - E]$, then we have $\varepsilon_v(P) = v(x_3) + m_4$*

Proof. The Kummer surface equation reduces modulo $\pi^{v(x_3)+v(x_4)+1}$ to

$$\begin{aligned} K(x_1,x_2,x_3,x_4) &\equiv (f_3^2 - 4f_2f_4)x_1^2x_3^2 - 2(2f_2x_1 + f_3x_2)x_1x_3x_4 \\ &\quad - 4f_2(f_5x_1 - f_6x_2)x_2x_3^2 + (f_1^2 - 4f_0f_2)x_1^4 \\ &\quad - 4f_0f_3x_1^3x_2 - 4f_0f_4x_1^2x_2^2 \\ &\equiv 0. \end{aligned}$$

Hence we see that $v(x_4) \geq m_4$ must hold. It is also easy to see that $\varepsilon_v(P) \geq v(x_3) + m_4$ holds.

First suppose $m_4 = m_3 - v(x_3)$. Then we have

$$\delta_3(x) \equiv 4(f_1^2 - 4f_0f_2)x_1^2(f_2x_1^2 + f_3x_1x_2 + f_4x_2^2) \pmod{\pi^{m_3+1}}$$

and it is a trivial check that this is not congruent to zero. Hence $\varepsilon_v(P) = m_3 = v(x_3) + m_4$ follows.

Similarly, if $m_4 = v(x_3) + v(f_6)$, then we get

$$\delta_1(x) \equiv 16f_2f_6x_3^2(f_2x_1^2 + f_3x_1x_2 + f_4x_2^2) \pmod{\pi^{2v(x_3)+v(f_6)+1}}$$

and thus $\varepsilon_v(P) = 2v(x_3) + v(f_6) = v(x_3) + m_4$.

In the situation $m_4 = \min\{v(x_3) + v(f_3^2 - 4f_2f_4), v(x_3) + v(f_5)\}$ we have to make a case distinction. From looking at the Kummer surface equation we know that at least two of the valuations of $(f_3^2 - 4f_2f_4)x_3, f_5x_3$ and x_4 must be equal. We have

$$\delta_2(x) \equiv x_1x_3\delta_2' \pmod{\pi^{v(x_3)+m_4+1}},$$

where

$$\begin{aligned}\delta_2' &= 5f_3x_1x_3(f_3^2-4f_2f_4)+4f_2f_5x_3(f_2x_1-3f_3x_2)-12f_2f_3x_1x_4\\ &\quad +2(8f_2f_4-5f_3^2)x_2x_4.\end{aligned}$$

If $m_4 = v((f_3^2-4f_2f_4)x_3) = v(f_5x_3) < v(x_4)$, then a short calculation using the Kummer surface equation reveals

$$\begin{aligned}\delta_2' &\equiv 5f_3x_1x_3(f_3^2-4f_2f_4)+4f_2f_5x_3(f_2x_1-3f_3x_2)\\ &\equiv f_2f_5x_2x_3(8f_3x_2+16f_2x_1)\\ &\equiv 8f_2f_5x_2x_3(f_3x_2+2f_2x_1)\\ &\equiv 16f_2f_5x_2x_3(1-x(P_2)) \pmod{\pi^{m_4+1}}\end{aligned}$$

and hence $\varepsilon_v(P) = v(x_3)+m_4$.

Now we assume $m_4 = v(f_5x_3) = v(x_4) \le v((f_3^2-4f_2f_4)x_3$. Here we substitute

$$5f_3x_1x_3(f_3^2-4f_2f_4) \equiv 5f_3(4f_2f_5x_2x_3+4f_2f_3x_1x_4+2f_3^2x_2x_4) \pmod{\pi^{m_4+1}}$$

in δ_2' and obtain

$$\begin{aligned}\delta_2' &\equiv 8f_2f_5x_3(f_3x_2+2f_2x_1)+8f_2x_4(f_3x_1+f_4x_2)\\ &\equiv 16f_2(x(P_2)-1)(f_5x_3-x_4) \pmod{\pi^{m_4+1}}.\end{aligned}$$

Hence assuming the incorrectness of the statement of the lemma implies

$$x_4 \equiv f_5x_3 \pmod{\pi^{m_4+1}}. \tag{A.15}$$

However, a very similar reasoning (namely, substituting $8f_2f_5f_3x_2x_3$ in δ_2') tells us that in this case we must also have

$$8f_2^2f_5x_3 \equiv (f_3^2-4f_2f_4)x_3. \tag{A.16}$$

Combining (A.15) and (A.16) gives a contradiction to the vanishing of the Kummer surface equation, which reduces to

$$K(x_1,x_2,x_3,x_4) \equiv f_5x_3 \equiv 0 \pmod{\pi^{m_4+1}}.$$

This completes the proof of Lemma A.1. □

Using a transformation of the curve we also get formulas for the value of ε_v on all components of the form $[C_i-A], [C_i-E]$ for $i \neq m_2/2$ and $[B_i-A], [B_i-E]$ for $i \neq m_1/2$.

What happens when P maps to $[D_{m_3/2}-A]$ (or $[D_{m_3/2}-E]$, which does not make a difference)? Then $v(x_4) \ge m_3/2$ and hence $v(\delta_i(x)) \ge m_3$ can be observed immediately. We find that

$$\varepsilon_v(P) = v(\delta_3(x)) = m_3 \tag{A.17}$$

using

$$\delta_3(x) \equiv -16f_0f_2f_4x_1^2x_2^2 + 4f_1^2(f_2x_1^2 + f_3x_1x_2 + f_4x_2^2)x_1^2 \pmod{\pi^{m_3+1}},$$

because the sum in parentheses can be easily seen not to be congruent to zero.

Finally we get $\varepsilon_v(P) = m_2$ (or $\varepsilon_v(P) = m_1$) for P mapping to $[C_{m_2/2} - A], [C_{m_2/2} - E]$ (or $[B_{m_1/2} - A], [B_{m_1/2} - E]$ respectively) using a suitable transformation applied to (A.17).

This completes the determination of $\varepsilon_v(P)$ for all components of the form $[B_i - A], [C_i - A], [D_i - A], [B_i - E], [C_i - E], [D_i - E]$.

Now suppose $P = [(P_1) - (P_2)]$ with $0 < v(x(P_1)) =: i < m_3/2$ and $0 < -v(x(P_2)) =: j < m_1/2$. In that case we have

$$\begin{aligned} x_1 &= \frac{1}{x(P_1) + x(P_2)}, \\ x_2 &= 1, \\ x_3 &= \frac{x(P_1)x(P_2)}{x(P_1) + x(P_2)}, \\ x_4 &= \frac{F_0(x(P_1), x(P_2)) + 2y(P_1)y(P_2)}{(x(P_1) - x(P_2))^2(x(P_1) + x(P_2))}. \end{aligned}$$

Hence we find $v(x_1) = j, v(x_2) = 0$ and $v(x_3) = i$. In order to determine $v(x_4)$, notice that we have $v(y(P_1)) = i$ and $v(y(P_2)) = -2j$; we write

$$x(P_1) = \pi^i x'(P_1), y(P_1) = \pi^i y'(P_1), x(P_2) = \pi^{-j} x'(P_2), y(P_2) = \pi^{-2j} y'(P_2).$$

Looking more closely at the blow-ups necessary to compute the minimal proper regular model of the curve, we see that $y'(P_1) \equiv \pm x'(P_1) \pmod{\pi}$ and $y'(P_2) \equiv \pm x'(P_2)^2 \pmod{\pi}$. In fact we have

$$\begin{aligned} P_1 \mapsto D_i &\Leftrightarrow y'(P_1) \equiv -x'(P_1) \pmod{\pi} \\ P_1 \mapsto D_{m_3-i} &\Leftrightarrow y'(P_1) \equiv x'(P_1) \pmod{\pi} \\ P_2 \mapsto B_j &\Leftrightarrow y'(P_2) \equiv x'(P_2)^2 \pmod{\pi} \\ P_2 \mapsto B_{m_1-j} &\Leftrightarrow y'(P_2) \equiv -x'(P_2)^2 \pmod{\pi}. \end{aligned}$$

Using

$$v(x_4) = v(F_0(x(P_1), x(P_2)) + 2y(P_1)y(P_2)) + 3j,$$

and

$$v(F_0(x(P_1), x(P_2)) + 2y(P_1)y(P_2)) \geq i - 2j$$

and the fact that we have

$$v(F_0(x(P_1), x(P_2)) + 2y(P_1)y(P_2)) > i - 2j$$

if and only if $y'(P_1)y'(P_2) \equiv x'(P_1)x'(P_2)^2 \pmod{\pi}$, we draw the conclusion that

$$v(x_4) = i + j = v(x_1) + v(x_3)$$

holds whenever we are in the situation $P \mapsto [D_i - B_j]$ or $P \mapsto [D_{m_3-i} - B_{m_1-j}]$. On the other hand, we see that

$$v(x_4) > i + j = v(x_1) + v(x_3)$$

holds for $P \mapsto [D_{m_3-i} - B_j]$ or $P \mapsto [D_i - B_{m_1-j}]$.

In both cases the inequality $v(\delta_i(x)) \geq v(x_1) + v(x_3)$ holds for all $i = 1, 2, 3, 4$, but in the former case we can compute $\varepsilon_v(P)$ easily, because then

$$\delta_2(x) \equiv 5f_3x_2^2x_4^2 - 10f_3^2x_1x_2x_3x_4 + 16f_2f_4x_1x_2x_3x_4 \pmod{\pi^{2v(x_4)+1}}$$

and

$$K(x_1, x_2, x_3, x_4) \equiv x_2^2x_4^2 - 2f_3x_1x_2x_3x_4 \pmod{\pi^{2v(x_4)+1}},$$

follow, similarly to (A.13). Therefore we deduce

$$\varepsilon_v(P) = v(x_1) + v(x_3) + v(x_4) = 2v(x_4) = 2i + 2j.$$

Recall the definition of m_5 given in the statement of Proposition 3.56. For the two remaining cases we show the following:

Lemma A.2. *Suppose P maps to $[D_{m_3-i} - B_j]$ or $[D_i - B_{m_1-j}]$. Then we have*

$$\varepsilon_v(P) = m_5.$$

Proof. The Kummer surface equation reduces to

$$\begin{aligned} K(x_1, x_2, x_3, x_4) &\equiv (f_3^2 - 4f_2f_4)x_1^2x_3^2 - 2f_3x_1x_2x_3x_4 - 4f_2f_5x_1x_2x_3^2 \\ &\quad - 4f_1f_4x_1^2x_2x_3 - 4f_0f_4x_1^2x_2^2 - 4f_6x_2^2x_3^2 \\ &\equiv 0 \pmod{\pi^{v(x_1)+v(x_3)+v(x_4)+1}}. \end{aligned}$$

Hence we see that $v(x_4) \geq m_5$ must hold.

First suppose that $m_5 = v(f_0x_1^2)$. Then we get $v(\delta_i(x)) \geq m_5$ for all i and

$$\varepsilon_v(P) = v(\delta_3(x)) = v(-16f_0f_2f_4x_1^2x_2^2) = m_5.$$

Similarly we find that

$$\varepsilon_v(P) = v(\delta_1(x)) = v(-16f_2f_4f_6x_2^2x_3^2) = m_5,$$

whenever $m_5 = v(f_6x_3^2)$.

Therefore we may reduce to the situation

$$m_5 = \min\{2v(x_4), v((f_3^2 - 4f_2f_4)x_1^2x_3^2), v(f_1x_1^2x_3^2), v(f_5x_1^2x_3^2)\}$$

and

$$\begin{aligned} K(x_1,x_2,x_3,x_4) &\equiv (f_3^2-4f_2f_4)x_1^2x_3^2-2f_3x_1x_2x_3x_4-4f_2f_5x_1x_2x_3^2 \\ &\quad -4f_1f_4x_1^2x_2x_3\equiv 0 \pmod{\pi^{v(x_1)+v(x_3)+v(x_4)+1}}. \end{aligned}$$

Now the easiest possibility is $m_5 = v((f_3^2-4f_2f_4)x_1^2x_3^2)$. Then we have $v(\delta_i(x)) \geq m_5$ for all i and moreover

$$\begin{aligned} \delta_2(x) &\equiv (5f_3^2-4f_2f_4)x_1^2x_3^2+(16f_2f_4-10f_3^2)x_1x_2x_3x_4 \\ &\quad -12f_3x_1x_2x_3(f_2f_5x_3+f_1f_4x_1) \\ &\equiv 2x_1x_3(f_3^2-4f_2f_4)(f_3x_1x_3-4x_2x_4) \pmod{\pi^{m_5+1}}, \end{aligned}$$

where the second congruence is due to the Kummer surface equation. Since we also know $v(x_4) > v(x_1)+v(x_3)$, we deduce

$$\varepsilon_v(P) = v(\delta_2(x)) = m_5.$$

The remaining case

$$m_5 = \min\{2v(x_4), v(f_1x_1^2x_3^2), v(f_5x_1^2x_3^2)\}$$

and

$$K(x) \equiv -2x_1x_2x_3(f_3x_4+2f_1f_4x_1+2f_2f_5x_3) \equiv 0 \pmod{\pi^{v(x_1x_3x_4)+1}}. \tag{A.18}$$

is slightly more difficult.

From (A.18) we obtain

$$\gamma := f_3x_4+2f_1f_4x_1+2f_2f_5x_3 \equiv 0 \pmod{\pi^{r+1}},$$

where $r = \min\{v(x_4), v(f_1x_1), v(f_5x_3)\}$. It turns out that we always have

$$v(\delta_i(x)) > \min\{v(x_4), v(f_1x_1), v(f_5x_3)\}$$

for all i, so we have to be more careful.

We first take a closer look at the Kummer equation. Because of our assumption

$$m_5 = \min\{2v(x_4), v(f_1x_1^2x_3^2), v(f_5x_1^2x_3^2)\}$$

it reduces to

$$\begin{aligned} K(x) \equiv{}& x_2^2x_4^2-4f_2x_1^2x_3x_4-4f_4x_1x_3^2x_4-2f_1f_2x_1^3-2f_3f_5x_1x_3^3 \\ &-4f_1f_5x_1x_2^2x_3-4f_0f_4x_1^2x_2^2-4f_6x_2^2x_3^2-2x_1x_2x_3\gamma \\ \equiv{}& 0 \pmod{\pi^{2r+1}}. \end{aligned}$$

Now we substitute

$$f_3x_4 \equiv -2f_1f_4x_1-2f_2f_5x_3 \pmod{\pi^{2r+1}}$$

in $f_3^2 K(x)$. We obtain

$$\begin{aligned} f_3^2 K(x) &\equiv 4x_2^2(f_2^2 f_4^2 x_1^2 + f_2^2 f_5^2 x_3^2 + (2f_2 f_4 - f_3^2) f_1 f_5 x_1 x_3) \\ &\equiv 4x_2^2(f_1 f_4 x_1 - f_2 f_5 x_3)^2 \equiv 0 \pmod{\pi^{2r+1}}, \end{aligned}$$

and hence

$$f_1 f_4 x_1 \equiv f_2 f_5 x_3 \pmod{\pi^{r+1}}. \tag{A.19}$$

In particular we have $v(f_1 x_1) = v(f_5 x_3) = v(x_4) = r$ because of $f_3 x_4 \equiv 2 f_1 f_4 x_1 \pmod{\pi^{r+1}}$.

Looking at the valuations of the $\delta_i(x)$, we find

$$\begin{aligned} v(\delta_1(x)) &= v(4 f_2 f_5^2 x_2^2 x_3^2) = 2v(x_4), \\ v(\delta_3(x)) &= v(4 f_2 f_5^2 x_2^2 x_3^2) = 2v(x_4), \\ v(\delta_4(x)) &> 2v(x_4). \end{aligned}$$

We see that γ appears in $\delta_2(x)$ with multiplicity $-6 f_3 x_1 x_2 x_3$, so that subtracting $3 f_3 K(x)$ from δ_2 yields:

$$\begin{aligned} \delta_2(x) \equiv\ & 2 f_2 x_2^2 x_4^2 + 8 f_1 f_4 x_1 x_2^2 x_4 + 8 f_2 f_5 x_2^2 x_3 x_4 \\ & + 4(4 f_2 f_4 - f_3^2) x_1 x_2 x_3 x_4 + 4 f_1 f_3 f_5 x_1 x_2^2 x_3 \\ & + 16(f_1 f_4^2 + f_2^2 f_5) x_1^2 x_3^2 \pmod{\pi^{r x_1 x_3 + 1}}. \end{aligned}$$

Therefore we get

$$v(\delta_2(x)) \geq \min\{2v(x_4), v(f_1 x_1^2 x_3^2), v(f_5 x_1^2 x_3^2)\}\} = m_5$$

and if we had $\varepsilon_v(P) > m_5$, then the following conditions would have to be satisfied simultaneously:

- $m_5 = v(f_1 x_1^2 x_3^2) = v(f_5 x_1^2 x_3^2) < 2v(x_4)$
- $v(f_1) = v(f_5)$
- $(f_1 f_4^2 + f_2^2 f_5) x_1^2 x_3^2 \equiv 0 \pmod{\pi^{v(f_1 x_1^2 x_3^2)+1}}$

Note that we have

$$(f_1 f_4^2 + f_2^2 f_5) x_1^2 x_3^2 \equiv f_2 f_5 x_1 x_3^2 (f_4 x_3 + f_2 x_1) \pmod{\pi^{v(f_1)+1}}$$

because of (A.19), so the last condition can only be satisfied if $x_1 + x_3 \equiv 0 \pmod{\pi^{v(x_1)+1}}$ which means that $x(P_1)x(P_2) \equiv -1 \pmod{\pi}$. But since ε_v is constant on components, it is easy to see that this special case cannot occur, finishing the proof of the lemma. □

Notice that we can eliminate $2v(x_4)$ from the definition of m_5, because at least two of the terms in that definition must be equal. This is important in practice, because it allows us to compute ε_v once we know the component itself and the valuations of the coefficients of f.

We must now look at the case $P \mapsto [D_{m_3/2} - B_j]$, first for $j \neq m_1/2$. The case $j = 0$ has already been treated (see (A.17)). We check the duplication polynomials and find $v(\delta_i(x)) \geq m_3 + 2v(x_1)$ for all $i \in \{1, 2, 3, 4\}$ and in particular

$$\delta_3(x) \equiv 4f_4(4f_0f_2 + f_1^2)x_1^2x_2^2 \pmod{\pi^{m_3+2v(x_1)+1}},$$

so that

$$\varepsilon_v(P) = v(\delta_3(x)) = m_3 + 2v(x_1)$$

follows. Using suitable transformations, we have also completed the cases $[D_{m_3/2} - B_j]$, $[B_{m_1/2} - C_j]$, $[B_{m_1/2} - D_j]$, $[C_{m_2/2} - B_j]$ and $[C_{m_2/2} - D_j]$.

The final case we have to consider is $v(x_1) \geq m_1/2, v(x_3) \geq m_3/2$, i.e. P maps to $[D_{m_3/2} - B_{m_1/2}]$. We find $v(\delta_i(x)) \geq m_1 + m_3$ for all i and the congruence

$$\delta_4(x) \equiv f_1^2f_5^2 + 16f_0f_2f_4f_6 - 4f_0f_2f_5^2 - 4f_1^2f_4f_6)x_2^4 \pmod{\pi^{m_1+m_3}}$$

implies

$$\varepsilon_v(P) = m_1 + m_3.$$

In order to deal with the cases $[D_{m_3/2} - C_{m_2/2}], [B_{m_1/2} - C_{m_2/2}], [B_{m_1/2} - D_{m_3/2}], [C_{m_2/2} - B_{m_1/2}]$ and $[C_{m_2/2} - D_{m_3/2}]$ we apply a suitable transformation as usual. □

A.8 Proof of Theorem 3.62

Proof. In the course of this proof we do not assume that $v(2) = 0$ holds from the beginning, although we will do so from some point onward. We assume, however, that the cases are exactly as stated in Section 3.4.4, so in particular we have $H = 0$ whenever $v(2) = 0$ holds. Note that if we have residue characteristic 2, it will never play a role which of the two cases (i) or (ii) we consider, see the end of Section 3.4.4.

The idea of the proof is, similar to the semistable case, to break the problem down into a number of cases that are tractable and then use the explicit expressions for the δ_i. It turns out that instead of looking at $\delta_2(x)$ we should consider $\delta_2'(x) = \delta_2(x) - 5f_3K(x)$, where $K(x)$ is the Kummer surface equation. Moreover we denote by $y = (y_1, y_2, y_3, y_4)$ a set of v-integral Kummer coordinates for $2P$ satisfying $v(y_i) = 0$ for some i.

Note that unless we have $\mathcal{K} = I_0$, at least one of the following must hold:

$$v(h_0) > 3l, v(h_1) > l, v(f_0) > 6l, v(f_1) > 4l, v(f_2) > 2l$$

This is crucial in some of the estimates, so we postpone the case $\mathcal{K} = I_0$ until the end of the proof.

We first assume $v(x_1) = 0, v(x_2) > 0$ and $0 \leq v(x_3) \leq 4l$. In order to figure out the valuation of x_4, we can either check the definition of x_4 or the Kummer surface equation. Both methods lead to the result $v(x_4) \leq \frac{1}{2}v(x_3)$. Hence we find

$$\begin{aligned}
\delta_1(x) &\equiv 4x_1x_4^3 \pmod{\pi^{3v(x_4)+1}} \\
\delta_2'(x) &\equiv 4x_2x_4^3 + 12f_3x_1x_3x_4^2 \pmod{\pi^{v(\delta_2'(x))+1}} \\
\delta_3(x) &\equiv 4x_3x_4^3 \pmod{\pi^{v(x_3)+3v(x_4)+1}} \\
\delta_4(x) &\equiv x_4^4 \pmod{\pi^{4v(x_4)+1}}.
\end{aligned}$$

Suppose we have $v(2) = 0$. Then we can conclude $\varepsilon_v(P) = 3v(x_4)$ and that we can find Kummer coordinates $y = (y_1, y_2, y_3, y_4)$ for $2P$ satisfying $v(y_1) = 0,\ v(y_2) \geq \min\{v(x_2),\ v(x_3) - v(x_4) + v(3)\} > 0,\ v(y_3) = v(x_3),\ v(y_4) = v(x_4)$, so that $\varepsilon_v(2P) = 3v(x_4)$ holds as well. Thus we obtain

$$\mu_v(P) = \sum_{n=0}^{\infty} 4^{-n-1}3v(x_4) = v(x_4). \tag{A.20}$$

If we have $v(2) > 0$, then we use an observation that will also be important later on, so we put it into a

Lemma A.3. *If $v(2) > 0,\ v(x_1) = 0,\ v(x_2) > 0$ and $0 \leq v(x_3) \leq 4l$, then we have*

$$\mu_v(P) = v(x_4).$$

Proof. A more detailed analysis of the $\delta_i(x)$ shows that we get

$$\min\{3v(x_4) + 2v(2), 4v(x_4)\} \leq \varepsilon_v(x) \leq 4v(x_4)$$

and if $\varepsilon_v(x) = v(\delta_1(x)) < 4v(x_4)$, then we find $v(y_1) = 0$ and $0 < v(y_4) < v(x_4)$, so $2P$ falls into the same case as P. For each point $Q \in J(k_v)$ let $x(Q)$ denote a set of integral Kummer coordinates for Q such that one of the $x(Q)_i$ is a unit. Then we see that applying δ repeatedly to Kummer coordinates $x(2^nP)$ decreases $v(x(2^nP)_4)$ at each step and hence yields some t such that $\varepsilon_v(2^tP) = 4v(x(2^tP)_4)$ and $\varepsilon_v(2^{t+1}P) = 0$. It follows that we have $\mu_v(2^tP) = v(x(2^tP)_4)$. By induction we get the desired result, because if $\mu_v(2^{n+1}P) = v(x(2^{n+1}P)_4)$, then we find

$$\begin{aligned}
\mu_v(2^nP) &= \frac{1}{4}\varepsilon_v(P) + \frac{1}{4}\mu_v(2^{n+1}P) \\
&= \frac{1}{4}\varepsilon_v(P) + \frac{1}{4}v(x(2^{n+1}P)_4) \\
&= \frac{1}{4}\varepsilon_v(P) + \frac{1}{4}(4v(x(2^nP)_4) - \varepsilon_v(2^nP)) \\
&= v(x(2^nP)_4).
\end{aligned}$$

□

Next we consider the situation $v(x_1) > 0,\ v(x_2) = 0,\ v(x_3) \leq 2l$. Since x needs to satisfy the Kummer equation, we find that $v(x_4) > v(x_3)$ follows (otherwise we would have $K(x) \equiv x_2^2 x_4^2 \pmod{\pi^{2v(x_4)+1}}$. We get the following congruences:

$$\begin{aligned}
\delta_1(x) &\equiv 4f_3 f_5^2 x_2 x_3^3 \pmod{\pi^{3v(x_3)+1}} \\
\delta_2'(x) &\equiv 0 \pmod{\pi^{3v(x_3)+1}} \\
\delta_3(x) &\equiv 4f_3^2 f_6 x_3^4 + 4x_3 x_4^3 + 4f_3 f_5 x_3^3 x_4 \pmod{\pi^{4v(x_3)+1}} \\
\delta_4(x) &\equiv f_3^2 f_5^2 x_3^4 \pmod{\pi^{4v(x_3)+1}}
\end{aligned}$$

If $v(2) = 0$, then we have

$$\varepsilon_v(P) = v(\delta_1(x)) = 3v(x_3)$$

and

$$v(y_1) = 0, v(y_2) > 0, v(y_3) > 0, v(y_4) = v(x_3) \leq 2l.$$

Now if $v(y_3) \leq 4l$, then we are in the case considered above, so the conclusion is

$$\mu_v(P) = \frac{1}{4}\mu_v(2P) + \frac{1}{4}\varepsilon_v(P) = \frac{1}{4}v(y_4) + \frac{3}{4}v(x_3) = v(x_3). \tag{A.21}$$

The case $v(y_3) > 4l$ will be dealt with later, because the situation differs for different reduction types. However, we shall see that in all possible cases (A.21) follows. In fact, we will see that for some reduction types (namely II and II^*) it is impossible to have $v(y_1) = 0$ and $v(y_3) > 2l$.

Conversely, suppose $v(2) > 0$. Then the proof of the formula $\mu_v(P) = v(x_3)$ is analogous to Lemma A.3.

The last case that we can cover simultaneously for all Kodaira types $\mathcal{K} \neq I_0$ is the case $v(x_1) = v(x_2) = 0 < v(x_3) \leq 2l$. Here it is easy to see that x_3 and x_4 must satisfy $v(x_3) = v(x_4)$. Suppose we have $v(2) = 0$. The $\delta_i(x)$ reduce to

$$\begin{aligned}
\delta_1(x) &\equiv 4(x_1x_4 - f_5x_2x_3)(x_4^2 - f_3f_5x_3^2) \pmod{\pi^{v(\delta_1(x))+1}}, \\
\delta_2'(x) &\equiv 4x_2x_4(x_4^2 + 3f_3f_5x_3^2) + 4x_1x_3(3x_4^2 + f_3f_5x_3^2) \pmod{\pi^{v(\delta_2(x))+1}}, \\
\delta_3(x) &\equiv 4x_3x_4(x_4^2 + f_3f_5x_3^2) \pmod{\pi^{v(\delta_3(x))+1}}, \\
\delta_4(x) &\equiv (x_4^2 - f_3f_5x_3^2)^2 \pmod{\pi^{v(\delta_4(x))+1}}.
\end{aligned}$$

The idea is to look at a representation of P as a divisor on the curve; namely let $P_1, P_2 \in C$ such that $P = [(P_1) - (P_2)]$. As usual, we also write v for the valuation extending v if the points are only defined over an extension. See Remark A.4 below. We suppose without loss of generality that we have $v(x(P_1)) = v(x_3) > 0$ and $v(x(P_2)) = 0$. It turns out that we get

$$x_4 \equiv ax(P_1) \pmod{\pi^{v(x_3)+1}}$$

and hence

$$\begin{aligned}
\delta_1(x) &\equiv ax(P_1)^3\left(a - x(P_2)^2\right)^2 \pmod{\pi^{3v(x_3)+1}} \\
\delta_2'(x) &\equiv 16a^2x(P_1)^3x(P_2)\left(a + x(P_2)^2\right) \pmod{\pi^{3v(x_3)+1}} \\
\delta_3(x) &\equiv 4a^2x(P_1)^4x(P_2)\left(a + x(P_2)^2\right) \pmod{\pi^{4v(x_3)+1}} \\
\delta_4(x) &\equiv a^2x(P_1)^4\left(a - x(P_2)^2\right)^2 \pmod{\pi^{4v(x_3)+1}}.
\end{aligned}$$

Therefore we are required to make yet another case distinction.

Case $x(P_2)^2 \not\equiv \pm a \pmod{\pi}$

This case is easy: We find

$$v(\delta_1(x)) = v(\delta_2'(x)) = 3v(x_3) = 3v(x_4)$$

and

$$v(\delta_3(x)) = v(\delta_4(x)) = 4v(x_3) = 4v(x_4).$$

Therefore

$$\varepsilon_v(P) = v(x_3) = v(x_4)$$

and

$$v(y_1) = v(y_2) = 0, v(y_3) = v(y_4) = v(x_3) = v(x_4)$$

follow. However, $2P$ again satisfies the condition of case $x(P_2)^2 \not\equiv \pm a \pmod{\pi}$ if and only if a and $x(P_2)$ satisfy a certain quartic polynomial in two variables. Hence we cannot yet finish the proof for this case, but need to discuss the two other possible cases first in order to give a formula for $\mu_v(P)$.

Case $x(P_2)^2 \equiv a \pmod{\pi}$

Here we have

$$v(\delta_1(x)) > 3v(x_4) = 3v(x_3) = v(\delta_2'(x))$$

and

$$v(\delta_3(x)) = 4v(x_4) = 4v(x_3) < v(\delta_4(x)).$$

This means that $2P$ satisfies

$$v(y_1) > 0 = v(y_2),\ v(y_3) = v(x_3) < v(y_4),$$

so because of $v(x_3) \leq 2l$, this is another case we have finished already, see (A.21).

Case $x(P_2)^2 \equiv -a \pmod{\pi}$

In this situation we find that

$$v(\delta_1(x)) = 3v(x_4) = 3v(x_3) < v(\delta_2'(x))$$

and

$$v(\delta_3(x)) > v(x_4) = 4v(x_3) = v(\delta_4(x)),$$

implying that $2P$ satisfies

$$v(y_1) = 0 < v(y_2), v(y_3) > v(x_3) = v(y_4).$$

We want to use (A.20) in order to conclude

$$\mu_v(2P) = v(y_4) = v(x_4)$$

and thus

$$\mu_v(P) = v(x_4),$$

so we need to check that $v(y_3) \leq 4l$ holds. Using (A.22) we find that

$$\frac{\delta_3(x)}{\delta_2(x)} \equiv \frac{1}{4}x(P_1) \pmod{\pi^{v(x_3)+1}},$$

whence we conclude

$$v(\delta_3(x)) - v(\delta_2(x)) \leq 2l$$

which immediately implies $v(y_3) \leq 4l$.

Remark A.4. Of course the P_i might only be defined over a possibly ramified quadratic extension of the ground field, but this does not affect our results, so we will not address this technical difficulty again. A different strategy leading to the same result is the following: Use the duplication polynomials directly to check that the conditions $v(x_1) = v(x_2) = 0 < v(x_3) = v(x_4) \leq 2l$ imply that $2P$ falls into the preceding case or into the first case considered above and that $\varepsilon_v(x) = 3v(x_4)$ holds. The desired results follows from this (and similar computations for the other cases that we have to consider), but the formulas are very long.

If we have $\mathrm{char}(\mathfrak{k}_v) = 2$, then the result follows upon observing $v(x_4) = v(x_3)$, $v(\delta_1(x)) > 3v(x_4), v(\delta_2'(x)) \geq 3v(x_4)$ and the congruences

$$\delta_3(x) \equiv (h_2x_3x_4 + f_3h_3x_3^2)^2 \pmod{\pi^{4v(x_3)+1}},$$

$$\delta_4(x) \equiv (x_4^2 + f_3f_5x_3^2)^2 \pmod{\pi^{4v(x_4)+1}}$$

combined with Lemma A.3.

From now on we assume that we are in the case $\mathrm{char}(\mathfrak{k}_v) \neq 2$. We show that in order for P to map to $\mathcal{J}_v^0$ the point must satisfy $v(x_4) \leq 2l$ in all situations we have not considered yet and then we can use what we have shown already. The proof for residue characteristic 2 follows the same pattern: One shows using the exact same methods that $v(x_4) \leq 2l$ must hold and we can finish the proof easily using Lemma A.3 or very similar statements. Therefore we have chosen to omit the details.

But now things start to get more complicated, because in order to deal with points satisfying $v(x_1) = 0,\ v(x_2) > 2l,\ v(x_3) > 4l + 1$ we need to consider the different Kodaira types separately. These are the cases where

the points P_i reduce to the same component C_i in the notation introduced above. See Remark A.4. We can safely disregard points satisfying $v(x_1) = 0 = v(x_2),\ v(x_3) > 2l$ or $v(x_1) > 0 = v(x_2),\ v(x_3) > 2l$ which were left out of the discussion so far, because they do not reduce to the connected component of the identity on the special fiber of the Néron model (which one could also show computationally by proving that such points are not in the image of the Jacobian under the respective multiplication maps), unless we are in a case of a reduction type having a trivial geometric component group. These reduction types are precisely II and II^*; however, according to our assumptions the coefficients of F must satisfy

$$v(f_0) = 6l + 1,\ v(f_1) \geq 4l + 1,\ v(f_2) \geq 4l + 1$$

in case II or

$$v(f_0) = 6l + 3,\ v(f_1) \geq 4l + 3,\ v(f_2) \geq 4l + 3$$

in case II^*, respectively. We thereby conclude that no point P_1 on the curve can satisfy $v(x(P_1)) > 2l$, so that we are completely done with these two cases already.

The next two reduction types in ascending order of size of Φ are III and III^* whose component groups have order 2. Therefore we do not have to put any further restriction on a point P satisfying $v(x_1) = 0, v(x_2) > 2l, v(x_3) > 4l + 1$ in order to ensure it reduces to $\mathcal{J}_v^0$.

If $\mathcal{K} = III$, then we have

$$v(f_0) \geq 6l + 1,\ v(f_1) = 4l + 1,\ v(f_2) \geq 4l + 1.$$

In fact we may assume $v(f_0) \geq 6l + 2$, since otherwise there are no points P of the present shape, see the discussion of type II. Looking at the Kummer equation we find that necessarily $0 < v(x_4) \leq 2l$ must hold, because otherwise

$$K(x) \equiv f_1^2 x_1^4 \pmod{\pi^{8l+3}}$$

leads to a contradiction. Hence we have

$$\begin{aligned} \delta_1(x) &\equiv 4x_1x_3^4 \pmod{\pi^{v(\delta_1(x))+1}}, \\ \delta_4(x) &\equiv 4x_4^4 \pmod{\pi^{v(\delta_4(x))+1}}; \end{aligned}$$

implying $v(\delta_1(x)) = 3v(x_4)$ and $v(\delta_4(x)) = 4v(x_4)$. Examining the other two duplication polynomials we also find $v(\delta_2'(x)) > 2l + 3v(x_4)$ and $v(\delta_3(x)) > 4l + 3v(x_4)$. We deduce

$$\varepsilon_v(P) = 3v(x_4)$$

and furthermore

$$\mu_v(P) = v(x_4) \tag{A.22}$$

using $v(y_1) = 0, v(y_2) > 2l, v(y_3) > 4l$ and $v(y_4) = v(x_4)$.

For the proof of the statement for reduction type III^* we first note that we cannot have points P_1 on the curve satisfying $v(x(P_1)) = 2l + 1$. This can be verified by tracing through the process of blowing up, since such a point would have to reduce to a component of multiplicity greater than 1 on the special fiber of $\mathcal{C}_v^{\min}$, which is absurd. Therefore we may assume $v(x(P_1)) \geq 2l + 2,\ v(x(P_2)) \geq 2l + 2$ so that $v(x_2) \geq 2l + 1,\ v(x_3) \geq 4l + 3$ and using

$$v(f_0) \geq 6l + 5, v(f_1) = 4l + 3, v(f_2) \geq 2l + 2$$

we find that

$$F(x(P_1), 1)) \equiv f_0 + f_1 x(P_1) \equiv 0 \pmod{\pi^{6l+6}}$$

and that

$$F(x(P_2), 1)) \equiv f_0 + f_1 x(P_2) \equiv 0 \pmod{\pi^{6l+6}}.$$

Therefore we deduce $v(x(P_1) - x(P_2)) \geq 2l + 3$ and $v(x_2^2 - 4x_1x_3) \geq 4l + 6$.

The Kummer equation reduces to

$$K(x) \equiv (x_2^2 - 4x_1x_3)x_4^2 + x_1^2(f_1^2x_1^2 - 4f_0x_1x_4 - 2f_1x_2x_4) \pmod{\pi^{6l+6+v(x_4)}},$$

so the vanishing of $K(x)$ implies $v(x_4) \leq 2l$ and hence the desired result $\mu_v(P) = v(x_4) \leq 2l$ follows in the same way as (A.22).

Reduction types IV and IV^*, being the only types that can have component groups of order 3, are only slightly more involved. Fortunately, there is an easy criterion that tells us when two points on the curve mapping to the components C_1 or C_2 map to the same component. This is completely analogous to the elliptic curve situation, see [16].

If we have reduction type IV, then we get

$$v(f_0) = 6l + 2,\ v(f_1) \geq 4l + 2,\ v(f_2) \geq 4l + 2$$

and moreover

$$y(P_1)^2 \equiv f_0 \pmod{\pi^{6l+3}}$$

for a point $P_1 \in C$ such that $v(x(P_1)) > 2l$. If we let $f_0 = \pi^{6l+2}f_0'$ and denote the two square roots of f_0' by α_1 and α_2, then P_1 maps to C_1, say, if and only if

$$y(P_1) \equiv \pi^{3l+1}\alpha_1,$$

and thus the point $P = [(P_1) - (P_2)] \in J(k_v)$ maps to $\mathcal{J}_v^0$ if and only if $v(x_1) = 0,\ v(x_2) > 2l,\ v(x_3) > 4l+1$ and $f_0 \equiv y(P_1)y(P_2) \pmod{\pi^{6l+3}}$. Assuming the first three conditions, the last condition is equivalent to $v(x_4) \leq 2l$ and we conclude

$$\varepsilon_v(P) = 3v(x_4)$$

and

$$\mu_v(P) = v(x_4)$$

as in the proof of (A.22).

The case of reduction type IV^* is similar, the only differences are that we now have

$$v(f_0) = 6l + 4,\ v(f_1) \geq 4l + 3,\ v(f_2) \geq 4l + 3$$

and that if P_1 is a point satisfying $v(x(P_1)) > 2l$, then for the same reason as in the case of type III^* the x-coordinate has valuation even greater than $2l + 1$, so that we can assume $v(x_1) = 0,\ v(x_2) > 2l + 1,\ v(x_3) > 4l + 3$ and

$$f_0 \equiv y(P_1)y(P_2) \pmod{\pi}^{6l+5}.$$

We get the same results

$$\varepsilon_v(P) = 3v(x_4)$$

and

$$\mu_v(P) = v(x_4).$$

If we are in case $\mathcal{K} = I_n^*$ for $n \geq 0$, then we have 4 components of simple multiplicity in the special fiber $\mathcal{C}_v^{\min}$ which we denote by C_1, C_2, C_3 and C_4. Here C_1 is the component that contains all points $P_1 = (x, y)$ satisfying $v(x) \leq 2l$ and the points at infinity. Recall that $F(X, Z) = F_1(X, Z)G(X, Z)$ such that $v(\mathrm{disc}(F_1)) > 0$ and both the discriminant of G and the resultant of F_1 and G have valuation equal to zero. In the present case we have

$$v(\mathrm{disc}(F)) = v(\mathrm{disc}(F_1)) = 12l + 6 + n$$

and

$$v(f_0) \geq 6l + 3,\ v(f_1) \geq 4l + 2,\ v(f_2) \geq 2l + 1.$$

Because of (A.20) we only need to check points $P = [(P_1) - (P_2)]$ such that P_1 and P_2 both map to the same component C_i, where $i > 1$. Our goal is to prove that in this situation we always have $v(x_4) \leq 2l$, because then the same proof as the one of (A.22) shows $\mu_v(P) = v(x_4) \leq 2l$.

We may assume that F_1 is of the form

$$F_1(X, Z) = x^3 + a_2X^2Z + a_1XZ^2 + a_0Z^3,$$

where $a_i \in \mathcal{O}_v$. We set

$$s(T) := T^3 + a_{2,1}T^2 + a_{1,2}T + a_{0,3},$$

where $a_i = a_{i,j}\pi^{(6-2i)l+j}$. Then we see that $v(\mathrm{disc}(s)) \geq 0$.

If $v(\mathrm{disc}(s)) = 0$, then we have $\mathcal{K} = I_0^*$. Note that we must have $v(f_0) = v(a_0) = 6l + 3$ or $v(f_1) = v(a_1) = 4l + 2$. In this case let

$$s(T) \equiv (T - t_2)(T - t_3)(T - t_4) \pmod{\pi}.$$

The components C_i for $i > 1$ are defined by $x' \equiv t_i \pmod{\pi}$, where $x(P_1) = x'\pi^{2l+1}$. Therefore the points $P \in J_0(k_v)$ are characterized among the points satisfying $v(x_1) = 0,\ v(x_2) \geq 2l+1,\ v(x_3) \geq 4l+2$ by

$$v(x_2^2 - 4x_1x_3) \geq 4l + 4.$$

We first prove a technical lemma. If we have $x(P_1) \neq x(P_2),\ v(x(P_1)) \geq 2l+c,\ v(x(P_2)) \geq 2l+c$ and $v(x(P_1) - x(P_2)) = N > 2l+c$ for some $c \geq 1$, then

$$v(F(x(P_1), 1) - F(x(P_2), 1)) \geq 4l + N + 1 + c$$

follows immediately. We now show that we can restrict our attention to the case where the inequality is strict.

Lemma A.5. *Suppose we are in case $\mathcal{K} = I_n^*$ such that $n \geq 0,\ x(P_1) \neq x(P_2),\ v(x(P_1)) \geq 2l+c,\ v(x(P_2)) \geq 2l+c$ and $v(x(P_1)-x(P_2)) = N > 2l+c$ for some $c \geq 1$.*
If $v(F(x(P_1), 1) - F(x(P_2), 1)) = 4l + N + 1 + c$, then we find $v(x_4) \leq 2l$.

Proof. We use the definition of x_4. We set $x_1 = 1$, and we get

$$x_4 = \frac{F_0(x(P_1), x(P_2)) + 2y(P_1)y(P_2)}{(x(P_1) - x(P_2))^2}.$$

But we have

$$\begin{aligned} &F_0(x(P_1), x(P_2)) \\ &= F(x(P_1), 1) + F(x(P_1), 1) + (x(P_1) - x(P_2))^2 M_0(x(P_1), x(P_2)), \end{aligned}$$

where

$$\begin{aligned} M_0(x(P_1), x(P_2)) \;=\; & f_2 + f_3(x(P_1) + x(P_2)) + f_4(x(P_1) + x(P_2))^2 \\ & + f_5(x(P_1) + x(P_2))(x(P_1)^2 + x(P_1)x(P_2) + x(P_2)^2) \\ & + f_6(x(P_1)^2 + x(P_1)x(P_2) + x(P_2)^2)^2. \end{aligned}$$

Thus we clearly have

$$M_0(x(P_1), x(P_2)) \equiv 0 \pmod{\pi^{2l+1}}$$

and it suffices to show that

$$v(F(x(P_1), 1) + F(x(P_2), 1)) + 2y(P_1)y(P_2))) \leq 4l + N + 1 + c \qquad \text{(A.23)}$$

in order to conclude

$$v(x_4) \leq 4l + N + 1 + c - 2N < 4l + 1 + c - (2l + c) = 2l + 1.$$

But this is easy: If $v(F(x(P_1), 1)) \neq v(F(x(P_2), 1))$, then we obtain

$$v(F(x(P_1), 1) + F(x(P_2), 1)) \leq 4l + N + 1 + c$$

and

$$v(y(P_1)y(P_2)) = \frac{v(F(x(P_1),1)) + v(F(x(P_2),1))}{2} > 4l + N + 1 + c,$$

proving (A.23).

If $v(F(x(P_1),1)) = v(F(x(P_2),1)) < 4l + N + 1 + c$, then (A.23) is obvious.

Finally, suppose $v(F(x(P_1),1)) = v(F(x(P_2),1)) = 4l + N + 1 + c$. Here we use

$$\begin{aligned} & (F(x(P_1),1) + F(x(P_2),1) + 2y(P_1)y(P_2))(F(x(P_1),1) + F(x(P_2),1) \\ & - 2y(P_1)y(P_2)) \\ = \; & (F(x(P_1),1) - F(x(P_2),1))^2 \end{aligned}$$

which implies (A.23) upon noticing that both factors on the left hand side have valuation at least equal to $4l + N + 1 + c$, whereas the valuation of the product equals $8l + 2N + 2 + 2c$. □

We now resume the proof of the theorem. Suppose we have a point satisfying $x(P_1) \neq x(P_2)$, $v(x(P_1)), v(x(P_2)) \geq 2l + 1$, $v(x(P_1) - x(P_2)) = N > 2l + 1$ and $v(F(x(P_1),1) - F(x(P_2),1)) > 4l + 2 + N$. Note that the last assumption yields

$$f_1 + 2f_2x(P_i) + 3f_3x(P_i)^2 \equiv 0 \pmod{\pi^{4l+3}} \tag{A.24}$$

for $i = 1, 2$.

Now we also have

$$F(x(P_i),1) \equiv 0 \pmod{\pi^{6l+4}}, \tag{A.25}$$

but (A.24) and (A.25) imply that s has a multiple root, contradicting $\mathcal{K} = I_0^*$.

We have omitted the case $x(P_1) = x(P_2)$ so far. We will have occasion to use

$$u(T) := f_3^2T^4 - 2f_3f_1T^2 - 8f_3f_0T + f_1^2 - 4f_0f_2. \tag{A.26}$$

In this situation we get

$$K(x) \equiv u(x(P_1)) - 4x_4F(x(P_1),1) \equiv 0 \pmod{\pi^{8l+4}}$$

and hence $v(x_4) > 0$ can only occur if $u(x(P_1)) \equiv 0 \pmod{\pi^{8l+4}}$.

A short calculation reveals that together with

$$F(x(P_1),1) \equiv 0 \pmod{\pi^{6l+4}}$$

this implies $v(\mathrm{disc}(s)) > 0$, a contradiction.

The case $\mathcal{K} = I_1^*$ is characterized by $v(\mathrm{disc}(s(T))) = 1$. Using a transformation we can assume that the double root of s is at zero, so we find that

$$v(f_0) = 6l + 4,\ v(f_1) \geq 4l + 3,\ v(f_2) = 2l + 1$$

and the component C_2 is given by $x' + a_2 \equiv 0 \pmod{\pi^{2l+2}}$. The other two components C_3 and C_4 are given by the distinct lines that are the components of $q(x') \pmod{\pi}$, where

$$q(T) = T^2 - a_{0,4} \pmod{\pi}$$

and $x(P_1) = x''\pi^{2l+2}$ (see [89, §IV.9]). This means that if a point $P = [(P_1)-(P_2)]$ maps to $\mathcal{J}_v^0$ such that $P_i \mapsto C_{3/4}$, then we have $v(x(P_i)) \geq 2l+2$ and

$$x(P_1) - x(P_2) \equiv 0 \pmod{\pi^{2l+3}}.$$

The proof of $v(x_4) \leq 2l$ for such points goes through as in the case of the analogous statement for $\mathcal{K} = IV$. Also notice that this works for reduction types I_n^* for odd n, because in such cases the components C_3 and C_4 are given by the components of $(x''')^2 - a_{0,3+n} \pmod{\pi}$, where $x(P_1) = x'''\pi^{2l+1+n}$.

What if we have $P = [(P_1) - (P_2)] \in J_0(k_v)$ and $P_i \mapsto C_2$? Then P satisfies $v(x_1) = 0, v(x_2) = 2l + 2, v(x_3) = 4l + 2$ as in the case $\mathcal{K} = I_0^*$. However, if $x(P_1) \neq x(P_2)$ and we set $N := v(x(P_1) - x(P_2))$, then we get

$$\begin{aligned} F(x(P_1),1) - F(x(P_2),1) \equiv\ & (x(P_1) - x(P_2))(f_1 + f_2(x(P_1) + x(P_2)) \\ & + f_3(x(P_1)^2 + x(P_1)x(P_2) + x(P_2)^2)) \\ \equiv\ & (x(P_1) - x(P_2))(f_1 + aa_2^2) \pmod{\pi^{4l+2+N}}, \end{aligned}$$

whereby we deduce that $v(F(x(P_1),1) - F(x(P_2),1)) = 4l + 2 + N$. Lemma A.5 proves that $v(x_4) \leq 2l$, allowing us to conclude $\mu_v(P) = v(x_4) \leq 2l$. This generalizes to the case of arbitrary odd integers $n \geq 1$.

If on the other hand $x(P_1) = x(P_2)$, where $v(x(P_1)) > 2l$, then we must have $P_1 \mapsto C_2$ (otherwise P_1 and P_2 do not map to the same component) and

$$K(x) \equiv u(x(P_1)) - 4x_4F(x(P_1),1) \equiv 0 \pmod{\pi^{8l+5}}.$$

But since in this situation we have

$$u(x(P_1)) \equiv f_3^2 x(P_1)^4 \pmod{\pi^{8l+5}},$$

we see directly that $\mu_v(P) = v(x_4) \leq 2l$ follows. This works for any $n \geq 1$.

Now we move on to the case $\mathcal{K} = I_2^*$, where we find that

$$v(f_0) = 6l + 5,\ v(f_1) \geq 4l + 3,\ v(f_2) = 2l + 1.$$

The component C_2 is as in the last case (and remains so for all $n \geq 1$) and the components C_3 and C_4 are given by the distinct lines that $r(T) = 0$ consists of, where

$$r(T) = a_{2,1}T^2 + a_{4,3}T + a_{0,5}.$$

It follows that if P_1 maps to $C_{3,4}$, then the valuation of $x(P_1)$ equals $2l+2$. If in addition $P = [(P_1) - (P_2)]$ maps to $\mathcal{J}^0(\mathfrak{k}_v)$, then we have $v(x(P_1) - x(P_2)) \geq 2l+3$.

Suppose $x(P_1) \neq x(P_2)$ and let $N := v(x(P_1) - x(P_2))$. We can use Lemma A.5 with $c = 2$ to deduce $v(x_4) \leq 2l$ if $v(F(x(P_1),1) - F(x(P_2),1)) = 4l + N + 3$. But in order to have

$$v(F(x(P_1),1) - F(x(P_2),1)) > 4l + N + 3,$$

we must have

$$f_1 + f_2(x(P_1) + x(P_2)) \equiv 0 \pmod{\pi^{4l+4}}$$

and hence $v(f_1) = 4l+3$. In this case however, assuming $v(x_4) > 2l$ leads to a contradiction, because then

$$K(x) \equiv f_1^2 x_1^4 \equiv 0 \pmod{\pi^{8l+7}}$$

holds.

Now we suppose $x(P_1) = x(P_2)$ and consider the Kummer surface equation

$$\begin{aligned} K(x) &\equiv -4F(x(P_1),1)x_4 + u(x(P_1)) \\ &\equiv -4F(x(P_1),1)x_4 + f_1^2 - 4f_0 f_2 \pmod{\pi^{8l+7}}. \end{aligned}$$

But

$$F(x(P_1),1) \equiv 0 \pmod{\pi^{6l+6}}$$

and $v(f_1^2 - 4f_0f_2) = 6l+6$ – recalling that we are in case I_n^* – together imply $v(x_4) \leq 2l$. A slight modification of this argument enables us to draw the same conclusion when $2|n$, $n \geq 4$, $P_1, P_2 \mapsto C_{3/4}$ and $x(P_1) = x(P_2)$ hold.

We are not done with the case $\mathcal{K} = I_2^*$ yet, because we have not looked at points $P = [(P_1) - (P_2)]$, where P_1 and P_2 map to C_2. We can assume P_1 and P_2 are distinct as the complementary case has been finished already for all $n \geq 1$.

If $v(f_1) = 4l+3$, then we can use the definition of x_4 directly:

$$\begin{aligned} F_0(x(P_1),x(P_2)) + 2y(P_1)y(P_2) &\equiv f_1(x(P_1) + x(P_2)) + 2y(P_1)y(P_2) \\ &\equiv 4y(P_1)y(P_2) \pmod{\pi^{6l+5}}. \end{aligned}$$

This congruence follows from

$$x(P_i) \equiv -a_2 \pmod{\pi^{2l+2}}$$

for $i = 1, 2$ and implies

$$v(x_4) = v(F_0(x(P_1),x(P_2)) + 2y(P_1)y(P_2)) - 2v(x(P_1) - x(P_2)) \leq 2l.$$

In the remaining case $v(f_1) > 4l + 3$ we can use Lemma A.5 with $c = 1$, because $N = v(x(P_1) - x(P_2))$ implies

$$\begin{aligned} &f_1 + f_2(x(P_1) + x(P_2)) + f_3(x(P_1)^2 + x(P_1)x(P_2) + x(P_2)^2)) \\ &\equiv aa_2^2 \pmod{\pi^{4l+3}} \end{aligned}$$

and so we have

$$v(F(x(P_1), 1) - F(x(P_2), 1)) = 4l + N + 2,$$

finishing the case I_2^*. In fact the same method covers all $P = [(P_1) - (P_2)]$ for the reduction types I_n^* where $P_i \in C_2$ and $n \geq 2$ is even.

Hence we have covered all possible situations for reduction types $\mathcal{K} = I_n^*$, $n \geq 1$. This means that we can finally move on to reduction type $\mathcal{K} = I_0$. Recall that we have

$$v(f_0) \geq 6l, v(f_1) \geq 4l, v(f_2) \geq 2l;$$

in the present case we have that at least one of the first two inequalities is actually an equality and the valuation of the discriminant equals $12l$. If we have $v(x(P_1)), v(x(P_2)) < 2l$, then the validity of the theorem is verified in the same way as the case $v(x(P_1)), v(x(P_2)) \leq 2l$ for the other reduction types. Moreover we see at once that the formulas given there prove

$$v(x_4) < 2l \text{ and } v(x_4) \leq v(x_3) \Rightarrow \mu_v(P) = v(x_4) \tag{A.27}$$

So we need to discuss the following cases:

(a) $v(x(P_1)) \geq 2l,\ 0 \leq v(x(P_2)) < 2l,\ v(x_4) \geq 2l$

(b) $v(x(P_1)) \geq 2l,\ v(x(P_2)) < 0,\ v(x_4) \geq 2l$

(c) $v(x(P_1)) \geq 2l,\ v(x(P_2)) \geq 2l,\ v(x_4) \geq 2l$

We consider these cases one after another, but we prove a preliminary result first. Compare this with Lemma A.3, which works for residue characteristic 2 and $\mathcal{K} \neq I_0$.

Lemma A.6. *For each point $Q \in J(k_v)$ let $x(Q)$ denote a set of integral Kummer coordinates for Q such that one of them is a unit. Suppose that there exists $t \geq 1$ such that $\varepsilon_v(2^n P) = 6l$ for $n \in \{1 \ldots, t-1\}$, but*

$$6l < \varepsilon_v(2^t P) \leq v(\delta_4(x(2^t P))) = 8l \leq v(\delta_3(x(2^t P))).$$

Then we have $\mu_v(P) = 2l$.

Proof. If $t = 1$, then we get

$$0 \leq v(x_4(P)) = v(\delta_4(x(P))) - \varepsilon_v(P) = 8l - \varepsilon_v(P) < 2l.$$

But (A.27) says that this implies $\mu_v(2P) = 8l - \varepsilon_v(P)$. Hence we find

$$\mu_v(P) = \frac{1}{4}\mu_v(2P) + \frac{1}{4}\varepsilon_v(P) = 2l \tag{A.28}$$

Now suppose $t > 1$. From (A.28) we deduce $\mu_v(2^t P) = 2l$. However, if $Q \in J(k)$ such that $\varepsilon_v(Q) = 6l$ and $\mu_v(2Q) = 2l$, then

$$\mu_v(Q) = \frac{1}{4}\mu_v(2Q) + \frac{1}{4}\varepsilon_v(Q) = \frac{1}{4}2l + \frac{1}{4}6l = 2l$$

follows, finishing the proof of the lemma. □

The obvious strategy is to show that in the present situation $\varepsilon_v(P) > 6l$ implies $v(\delta_4(x)) = 8l$. If that is the case we can combine Lemma A.6 with (A.27) and conclude $\mu_v(P) = \min\{v(x_4), 2l\}$. Recall the notation

$$u(T) = a^2T^4 - 2af_1T^2 - 8af_0T + f_1^2 - 4f_0f_2.$$

Lemma A.7. *If $v(T) \geq 2l$, then we cannot simultaneously have*

$$F(T, 1) \equiv 0 \pmod{\pi^{6l+1}}$$

and

$$u(T) \equiv 0 \pmod{\pi^{8l+1}}.$$

Proof. The proof consists of a simple algebraic verification showing that if the assumptions were satisfied, then the valuation of the discriminant of C would have to be larger than $12l$. □

Case (a)
Suppose that we have $v(x(P_1)) \geq 2l, 0 \leq v(x(P_2)) < 2l$, so that we have $v(x_1) = 0, 0 \leq v(x_2) < 2l, v(x_3) \geq 2l$. Then we get

$$v(x_4) \geq 2l, v(\delta_1(x)) \geq 6l, v(\delta_2(x)) \geq 6l, v(\delta_3(x)) \geq 8l \text{ and } v(\delta_4(x)) \geq 8l.$$

More precisely, if we set $x_1 = 1$, then we have

$$\begin{aligned}
\delta_1(x) &\equiv 4(a - x_2^2)^2 F(x_4/a, 1) \pmod{\pi^{6l+1}} \\
\delta_2(x) &\equiv 16ax_2(x_2 - 1)(x_2 - a)F(x_4/a, 1) \pmod{\pi^{6l+1}} \\
\delta_3(x) &\equiv 4x_2(x_2 - 1)(x_2 - a)u(x_4/a) \pmod{\pi^{8l+1}} \\
\delta_4(x) &\equiv (a - x_2^2)^2(x_2 - a)u(x_4/a) \pmod{\pi^{8l+1}}.
\end{aligned}$$

Hence Lemma A.7 shows that $\varepsilon_v(P) > 6l$ implies $v(\delta_4(x)) = 8l$.

Case (b)
If $v(x(P_1)) \geq 2l,\ v(x(P_2)) < 0$, then we must have $v(x_1) > 0,\ v(x_2) = 0,\ v(x_3) \geq 2l$. It follows that we have $v(x_4) > 2l,\ v(\delta_2(x)) > 6l$ and $v(\delta_3(x)) > 8l$. Moreover, setting $x_2 = 1$ yields

$$\begin{aligned} \delta_1(x) &\equiv a^2 F(x_3, 1) \pmod{\pi^{6l+1}}, \\ \delta_4(x) &\equiv u(x_3) \pmod{\pi^{8l+1}}. \end{aligned}$$

Thus we conclude that $\varepsilon_v(P) > 6l$ implies $v(\delta_4(x)) = 8l$ from Lemma A.7. Notice that the above contains $P_2 = \infty^{\pm}$ or $P_2 = \infty$ as a special case.

Case (c)
Finally we consider the case $v(x(P_1)) \geq 2l,\ v(x(P_2)) \geq 2l$. We have $v(x_1) = 0,\ v(x_2) \geq 2l$ and $v(x_3) \geq 4l$. It follows that $v(x_4) \geq 2l$ and $v(\delta_1(x)) \geq 6l,\ v(\delta_2(x)) \geq 8l,\ v(\delta_3(x)) \geq 10l,\ v(\delta_4(x)) \geq 8l$. In particular we can set $x_1 = 1$ to obtain

$$\begin{aligned} \delta_1(x) &\equiv 4a^2 F(x_4/a, 1) \pmod{\pi^{6l+1}} \\ \delta_4(x) &\equiv u(x_4/a) \pmod{\pi^{8l+1}} \end{aligned}$$

which finishes the proof of the theorem. □

A.9 Proof of Theorem 3.74

Proof. If $v(x_3) = 0$, then we can copy the part of the proof of Theorem A.8 that deals with the case $l = 0$. It was only given for the case of non-multiplicative $\mathcal{K}$; however, it remains valid for multiplicative $\mathcal{K}$ as well under the assumptions of the theorem.

In any case, we only have to consider points satisfying $v(x_3) > 0$. For such points we first prove the theorem for non-multiplicative $\mathcal{K}$. The case $v(x_1) = 0$ basically reduces to the analogous situation we have encountered in the proof of Theorem 3.62; so the proof that $\mu_v(P)$ is equal to $v(x_4)$ given there remains valid upon noticing that neither the coefficient f_5 nor, in case $\mathrm{char}(\mathfrak{k}_v)$, the expression $f_3(f_3+1)$ (which now have positive valuation) make a difference.

Hence we suppose that $v(x_1) > 0$ which implies that we must have $v(x_2) = 0$ and in addition $v(x_3) \leq 2l$ unless $\mathcal{K} = I_0$, a case we leave until the end of the proof. So we assume that $\mathcal{K}$ is an additive Kodaira type, which amounts to $v(f_2) > 2l,\ v(f_1) > 4l,\ v(f_0) > 6l,\ v(h_1) > l$ and $v(h_0) > 3l$ after a transformation, and $0 < v(x_3) \leq 2l$.

First we look at points satisfying $v(x_1) < m_1/2$. We find that

$$K(x) \equiv (f_3 x_1 x_3 - x_2 x_4 + h_2^2 x_1 x_3^2 x_4)^2 \pmod{\pi^{2v(x_1 x_3)+1}},$$

therefore we have

$$v(x_4) = v(x_1) + v(x_3)$$

and

$$v(f_3x_1x_3 + x_2x_4) = v(x_4).$$

Now we get the following congruences:

$$\begin{aligned}
\delta_1(x) &\equiv 4x_1x_4^3 - 4f_5x_3x_4(x_2x_4 + f_3x_1x_3) - 4f_3(4f_4f_6 - f_5^2)x_2x_3^3 \\
&\quad (\mathrm{mod}\ \pi^{\min\{4v(x_1),m_1\}+3v(x_3)+1}) \\
\delta_2'(x) &\equiv 8f_3f_4x_1x_3^2x_4 \pmod{\pi^{2v(x_1)+3v(x_3)+1}} \\
\delta_3(x) &\equiv (4f_4 + h_2^2)x_3^2x_4^2 \pmod{\pi^{2v(x_1)+4v(x_3)+1}} \\
\delta_4(x) &\equiv x_4^4 - f_3^2(h_2^2f_6 + 4f_4f_6 - f_5^2)x_3^4 \pmod{\pi^{\min\{4v(x_1),m_1\}+4v(x_3)+1}}
\end{aligned}$$

So we always have $v(\delta_3(x)) = 2v(x_1) + 4v(x_3)$. If $v(2) = 0$, then we get

$$\varepsilon_v(P) = v(\delta_2'(x)) = 2v(x_1) + 3v(x_3)$$

and if $v(2) > 0$, we find that

$$2v(x_1) + 3v(x_3) < \varepsilon_v(P) \leq 2v(x_1) + 4v(x_3).$$

The crucial observation is that if y is a set of integral Kummer coordinates of $2P$ containing a unit, then we know some of the valuations of the y_i, because we know what the points lying on the component $\chi(2P) = (\chi_1(2P), 0)$ look like. Namely, if $v(x_1) < m_1/4$, then $\chi_2(2P) = 2v(x_1)$ and hence

$$v(y_1) = 2v(x_1),\ v(y_2) = 0,\ v(y_3) \geq 0,\ v(y_4) \geq 0.$$

Because of $\mathcal{K} \neq I_0$, we also have $v(y_4) \leq 2l$. So in that case we get for residue characteristic not equal to 2

$$v(y_3) = v(x_3) \text{ and } v(y_4) = 2v(x_1) + v(x_3)$$

and in the complementary case we obtain $\varepsilon_v(P) = v(\delta_2'(x)) = 2v(x_1) + 3v(x_3) + r$, where r is positive, and hence

$$v(y_3) = v(x_3) - r \text{ and } v(y_4) = 2v(x_1) + v(x_3) - r.$$

If we have $m_1/4 \leq v(x_1) < m_1/2$, then $\chi_1(P) = m_1 - 2v(x_1)$, and so we have, similarly, $v(y_1) = m_1 - 2v(x_1),\ v(y_2) = 0,\ v(y_3) = v(x_3),\ v(y_4) = m_1 - 2v(x_1) + v(x_3)$ if $v(2) = 0$. In the other case we have $\varepsilon_v(P) = v(\delta_2'(x)) = 2v(x_1) + 3v(x_3) + r$ and $v(y_1) = m_1 - 2v(x_1),\ v(y_2) = 0,\ v(y_3) = v(x_3) - r,\ v(y_4) = m_1 - 2v(x_1) + v(x_3) - r$.

Now we consider points satisfying $v(x_1) \geq m_1/2$. Since in such cases the assumption $v(x_4) < m_1/2 + v(x_3)$ leads to the contradictory statement

$$K(x) \equiv x_2^2x_4^2 \equiv 0 \pmod{\pi^{2v(x_4)+1}},$$

we have

$$v(x_4) \geq m_1/2 + v(x_3).$$

Note that we know $v(y_1) = 0,\ v(y_2),\ v(y_3),\ v(y_4) \geq 0$, so in particular $\varepsilon_v(P) = v(\delta_1(x))$. It follows that we have

$$\begin{aligned}\delta_1(x) &\equiv -4f_3(4f_4f_6 - f_5^2)x_2x_3^3 \pmod{\pi^{m_1+3v(x_3)+1}}\\ \delta_4(x) &\equiv -f_3^2(4f_4f_6 - h_2^2f_6 - f_5^2)x_3^4 \pmod{\pi^{m_1+4v(x_3))+1}}\end{aligned}$$

which means that $\varepsilon_v(P) = v(\delta_1(x)) = m_1 + 3v(x_3) + r$, where $r \geq 0$ vanishes if the residue characteristic is not 2 and otherwise r is positive and $v(\delta_4(x)) = m_1 + 4v(x_3)$. Furthermore we find $v(\delta_2'(x)) \geq m_1 + 3v(x_3)$ and $v(\delta_3(x)) \geq m_1 + 4v(x_3)$. Notice that this implies $\mu_v(P) = m_1 + v(x_3)$ in both cases.

Combining all of these results, we can now slightly modify the proof of Lemma 3.49 to find the first summand $\frac{w_1(P)(m_1 - w_1(\check{P}))}{m_1}$. For $v(2) = 0$, we can then combine this with the fact that the valuation of the third Kummer coordinate does not change if we normalize the coordinates at each step; if $v(2) > 0$, then we use the fact that we have $\varepsilon_v(P) = 2w_1(P) + 3v(x_3) + r$, but $v(y_3) = v(x_3) - r$, so the proof of Lemma A.3 applies in this case. This proves the theorem for all reduction types $\mathcal{K} \neq I_0$

It remains to verify the correctness of the theorem for $\mathcal{K} = I_0$. For this we again assume $\mathrm{char}(\mathfrak{k}_v) \neq 2$, because the complementary case is similar. The case $v(x_1) = 0$ reduces to the analogous situation in Theorem 3.62 and if $v(x_3) < 2l$, we can simply copy the proof given for the other reduction types above, so we can reduce to the case where $v(x_1)$ is positive and $v(x_3) \geq 2l$. Checking the Kummer surface equation tells us that we must have

$$v(x_4) \geq \min\{v(x_1), m_1/2\} + 2l.$$

Suppose that $v(x_1) < m_1/2$. We show that $\varepsilon_v(P) \geq 2v(x_1) + 6l$ holds and that $\varepsilon_v(P) > 2v(x_1) + 6l$ implies $v(\delta_3(x)) = 8l + 2v(x_1)$. Consider

$$\begin{aligned}\delta_2'(x) &\equiv -16x_1^2F(x_3, 1) \pmod{\pi^{2v(x_1)+6l+1}},\\ \delta_3(x) &\equiv 4f_4x_1^2u(x_3) \pmod{\pi^{2v(x_1)+8l+1}},\end{aligned}$$

where u was defined in (A.26).

As in Lemma A.7 we can now show easily that we cannot have both $v(F(x_3, 1)) > 6l$ and $v(u(x_3)) > 8l$, proving that $\varepsilon_v(P) > 2v(x_1) + 6l$ indeed implies $v(\delta_3(x)) = 8l + 2v(x_1)$.

In fact this suffices for our purposes, because we know that

$$v\left(\frac{\delta_1(x)}{\delta_2'(x)}\right) \geq \min\{2v(x_1), m_1 - 2v(x_1)\};$$

here equality holds unless possibly when $v(x_1) = m_1/4$. Moreover, it is easy to see that we have

$$v\left(\frac{\delta_4(x)}{\delta_2'(x)}\right) \geq v(\delta_1(x)) + 2l.$$

Finally, suppose $v(x_1) \geq m_1/2$. This yields

$$\begin{aligned} \delta_1(x) &\equiv (f_5^2 - 4f_6)F(x_3, 1) \pmod{\pi^{m_1+6l+1}} \\ \delta_4(x) &\equiv 4(f_5^2 - 4f_6)u(x_3) \pmod{\pi^{m_1+8l+1}}. \end{aligned}$$

We can also show $v(\delta_2'(x)) \geq m_1 + 6l$ and $v(\delta_3(x)) \geq m_1 + 8l$, so $\varepsilon_v(P) \geq m_1 + 6l$ holds and moreover $\varepsilon_v(P) > m_1 + 6l$ implies $v(\delta_4(x)) = 8l + m_1$.

Why does this finish the proof for the present reduction type? The methods used so far show that if we have $v(x_1) > 0$ and $v(x_3) \geq 2l$ then either $\varepsilon_v(P) = 2w_1(P) + 6l$ and the normalized third Kummer coordinate has valuation equal to $2l$, or we have $2w_1(P) + 6l \leq \varepsilon_v(P) \leq 2w_1(P) + 8l$ in which case we get $v\left(\frac{\delta_3(x)}{\delta_1(x)}\right) < 2l$ and hence

$$\mu_v(2P) = \frac{w_1(2P)(m_1 - w_1(2P))}{m_1} + v\left(\frac{\delta_3(x)}{\delta_1(x)}\right).$$

Now it is easy to see that this implies the desired formula for $\mu_v(P)$ and therefore for any P such that $v(x_1) > 0$, $v(x_3) \geq 2l$ and $\exists t \geq 1$ satisfying $\varepsilon_v(2^t P) > 2w_1(2^t P) + 6l$, but $\varepsilon_v(2^s P) = 2w_1(2^s P) + 6l$ for any $s = 1, \ldots, t-1$ using an induction-type argument as in the proof of Lemma A.6. If no such t exists, then the theorem is obvious from what has been proved already.

The last possible reduction type is $[I_{m_1} - I_{m_2} - l]$ where $l, m_1, m_2 > 0$. Suppose $v(2) = 0$; once again there is virtually no difference in the situation of residue characteristic 2.

In this case we may assume $v(f_2) = 2l$ and $v(f_0) - 6l \neq 2v(f_1) - 4l$. As before, we write

$$f_2 = f_2'\pi^{2l},\ f_4 = f_4'\pi^{4l},\ f_6 = f_6'\pi^{6l}$$

which means that we have

$$m_2 = \min\{v(f_0'), 2v(f_1')\} = \min\{v(f_0) - 6l, 2v(f_1) - 4l\}.$$

The proof for the case $v(x_1) \geq 0$ and $0 < v(x_3) < 2l$ can be copied verbatim from the verification of the theorem for $v(x_1) = 0, v(x_3) \leq 2l$ and additive $\mathcal{K}$. Note that our assumptions rule out the possibility that $v(x_1) > 0$ and $v(x_3) > 2l$.

Since we have $v(f_2) = 2l$ now, we need to verify the desired formula for $v(x_3) = 2l$ separately. However, in that case we may simply copy the respective proof for $\mathcal{K} = I_0$ upon noticing

$$F(x_3, 1) \equiv f_2 x_3^2 + f_3 x_3^3 \pmod{\pi^{6l+1}}$$

and

$$u(x_3) \equiv f_3^2 x_3^4 \pmod{\pi^{8l+1}},$$

so we certainly cannot have $v(u(x_3)) > 8l$.

It remains to consider the case $P \in J_0(k_v)$ such that both $v(x_1) = 0$ and $v(x_3) > 2l$. In order to have $P \in J_0(k_v)$ one of the following must hold:

1. $v(x(P_1)) \geq 2l,\ v(x(P_2)) \leq 2l$
2. $2l < v(x(P_1)) = v(x(P_2)) < 2l + m_2/2$
3. $v(x(P_1)) \geq 2l + m_2/2, v(x(P_2)) \geq 2l + m_2/2$

In the first case we have $2l < v(x_3) \leq 4l$ and

$$K(x) \equiv (x_2x_4 - f_3x_1x_3)^2 - 4x_1x_3x_4^2 - 4f_2x_1^2x_3x_4 \pmod{\pi^{8l+4i+1}}.$$

If we assume that $v(x_4) > 2l$, then $v(x_3) - v(x_2) \leq 2l$ implies that $K(x)$ reduces to $f_3^2x_1^2x_3^2$ which is absurd; hence we conclude $v(x_4) \leq 2l$.

Suppose

$$v(x(P_1)) = v(x(P_2)) = 2l + i < 2l + m_2/2,$$

then we have

$$K(x) \equiv (x_2^2 - 4x_1x_3)x_4^2 - 4x_1x_3x_4^2 - 4f_2x_1^2x_3x_4 \pmod{\pi^{8l+4i+1}}.$$

It follows that we have either $v(x_4) \leq 2l$ or $v(x_4) = 2l + 2i$. We want to show that the latter cannot occur. By assumption the points P_1 and P_2 are affine, so we can set $x_1 = 1$.

Since $v(x(P_2)) = 2l + i$, we have

$$y(P_i)^2 = F(x(P_i), 1) \equiv f_2x(P_i)^2 \pmod{\pi^{6l+2i+1}};$$

thus $v(y(P_1)) = v(y(P_2)) = 3l + i$ and

$$\begin{aligned} &F_0(x(P_1), x(P_2)) + 2y(P_1)y(P_2) \\ &\equiv f_2x(P_1)x(P_2) + 2y(P_1)y(P_2) \pmod{\pi^{6l+2i+1}} \end{aligned}$$

follow.

But we find $v(f_2x(P_1)x(P_2) + 2y(P_1)y(P_2)) = 6l + 2i$, because we have

$$\begin{aligned} &(f_2x(P_1)x(P_2) + 2y(P_1)y(P_2))^2 \\ &\equiv 2f_2x(P_1)x(P_2)(f_2x(P_1)x(P_2) + 2y(P_1)y(P_2)) \pmod{\pi^{6l+2i+1}}. \end{aligned}$$

So we must have $v(x_4) \leq 2l$.

In the remaining case $v(x(P_1)), v(x(P_2)) \geq 2l + m_2/2$ we find that the assumption $v(x_4) > 2l$ implies

$$K(x) \equiv (f_1^2 - 4f_0f_2)x_1^4 \pmod{\pi^{8l+m_2+1}}$$

which is yet another contradiction. Therefore we get $v(x_4) \leq 2l$ in this case as well.

The proof of the theorem is now completed using the observation that $\mu_v(P) = v(x_4)$ follows from $v(x_4) \leq 2l < v(x_3)$ as in the proof of Theorem 3.62 for $\mathcal{K} = I_0$, where the cases $v(x_4) < 2l$ and $v(x_4) = 2l$ (as a special case of $v(x_4) \geq 2l$) are treated separately. □

Bibliography

[1] W.W. Adams and P. Loustaunau, *An introduction to Gröbner bases*, American Mathematical Society, Providence (1994).

[2] M. Artin, *On isolated rational singularities of surfaces*, Amer. J. Math. **88**, 129–136 (1966).

[3] M. Artin, *Lipman's proof of resolution of singularities for surfaces*, in *Arithmetic geometry* [25], 267–287.

[4] D. Bernardi, *Hauteur p-adique sur les courbes elliptiques*, Seminar on number theory Paris 1979–1980, Progr. Math. **12**, Birkhäuser, Boston, 1–14 (1981).

[5] B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218**, 79–108 (1965).

[6] C. Birkenhake, H. Lange, *Complex Abelian Varieties*, 2nd edition, Springer-Verlag, Berlin (2004).

[7] A. Bobenko, B. Deconinck, M. Heil, M. Schmies and M. van Hoeij, *Computing Riemann Theta Functions*, Math. Comp., **73**, 1417–1442 (2004).

[8] E. Bombieri and W. Gubler, *Heights in diophantine geometry*, Cambridge University Press, Cambridge (2006).

[9] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Springer-Verlag, Berlin (1990).

[10] S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math. **98**, 275–293 (1999).

[11] J.-B. Bost and J.-F. Mestre, *Moyenne arithmético-géométrique et périodes des courbes des genre 1 et 2*, Gaz. Math. Soc. France **38**, 36–64 (1988).

[12] J.-B. Bost and J.-F. Mestre, *Calcul de la hauteur archimédienne des points d'une courbe elliptique par un algorithme quadratiquement convergent et application au calcul de la capacité de l'union de deux intervalles*, unpublished manuscript (1993).

[13] N. Bruin and M. Stoll, *The Mordell-Weil Sieve: Proving non-existence of rational points on curves*, LMS J. Comput. Math. **13**, 272–306 (2010).

[14] Y. Bugeaud, M. Mignotte, S. Sikseki, M. Stoll and S. Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory **8**, 859–885 (2008).

[15] J. Buhler, B.H. Gross and D. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Comp. **44**, 473-481 (1985).

[16] V. Busch, *Effektive Berechnung von Néron-Tate Höhen mittels Arakelov-Schnittzahlen*, Diploma thesis, Universität Hamburg (2008).

[17] V. Busch, *A refined version of the Tate algorithm*, Preprint (2009).

[18] V. Busch and J.S. Müller, *Local heights on elliptic curves and intersection multiplicities*, Preprint (2010). arXiv:math/1003.2500v1 [math.NT]

[19] D. Cantor, *Computing in the Jacobian of a Hyperelliptic Curve*, Math. Comp. **48, no. 177**, 95–101 (1987).

[20] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, Cambridge University Press, Cambridge (1996).

[21] T. Chinburg, *Minimal models for curves over Dedekind rings*, in *Arithmetic geometry* [25] 209–326.

[22] A. Clebsch, *Theorie der binären algebraischen Formen*, B. G. Teubner, Leipzig (1872).

[23] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin (1993).

[24] B. Conrad, *Minimal models for elliptic curves*, unpublished manuscript (2005).

[25] G. Cornell and J.H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York–Heidelberg–Berlin (1986).

[26] D. A. Cox and S. Zucker, *Intersection numbers of sections of elliptic surfaces*, Invent. Math. **53**, 1–44 (1969).

[27] J. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge (1996).

[28] J.E. Cremona, M. Prickett and S. Siksek, *Height difference bounds on elliptic curves over number fields*, J. Number Theory **116**, 42–68 (2006).

[29] B. Deconinck, M. van Hoeij, *Computing Riemann matrices of algebraic curves*, Physica D, **152–153**, 28-46 (2001).

[30] B. Deconinck and M. Patterson, *Computing the Abel map*, Physica D, **237**, 3214–3232 (2008).

[31] B. Deconinck, personal communication.

[32] S. Duquesne, *Calculs effectifs des points entier et rationnels sur les courbes*, Thèse de doctorat, Université Bordeaux (2001).

[33] S. Duquesne, *Traces of the group law on the Kummer surface of a curve of genus 2 in characteristic 2*, Preprint (2007).

[34] S. Duquesne, *Montgomery Ladder for all Genus 2 Curves in Characteristic 2,* Lecture Notes in Computer Sciences **5130**, 174–188 (2008).

[35] `ftp://megrez.math.u-bordeaux.fr/pub/duquesne`.

[36] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York (1995).

[37] G. Faltings, *Calculus on arithmetic surfaces*, Ann. of Math. (2) **119**, 387–424 (1984).

[38] J.-C. Faugère, *A new efficient algorithm for computing Grbner bases (F4)*, J. Pure Appl. Algebra **139** (1), 61–88 (1999).

[39] T. Fisher, *A new approach to minimising binary quartics and ternary cubics*, Math. Res. Lett. **14**, Issue 4, 597–613 (2007).

[40] E.V. Flynn, *The jacobian and formal group of a curve of genus 2 over an arbitrary ground field*, Math. Proc. Camb. Phil. Soc. 107, 425–441 (1990).

[41] E.V. Flynn, *The group law on the jacobian of a curve of genus 2*, J. reine angew. Math. **439**, 45–69 (1993) .

[42] E.V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc. **347**, 3003–3015 (1990).

[43] E.V. Flynn and N.P. Smart, *Canonical heights on the Jacobians of curves of genus* 2 *and the infinite descent*, Acta Arith. **79**, 333–352 (1997).

[44] E.V. Flynn, F. Leprévost, E.F. Schaefer, W.A. Stein, M. Stoll and J.L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70**, 1675–1697 (2001).

[45] P. Gaudry, *Fast genus 2 arithmetic based on Theta functions*, J. Math. Crypt. **1**, 243–265 (2007).

[46] B. Gross, *Local heights on curves*, in G. Cornell and J.H. Silverman (eds.), *Arithmetic geometry* [25], 327–339.

[47] A. Hashemi and D. Lazard, *Almost polynomial complexity for zero-dimensional Gröbner bases*, in Proceedings of the 7th Asian Symposium on Computer Mathematics (ASCM'2005), Seoul, Korea, 16–21 (2005).

[48] F. Hess, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comp. **33(4)**, 425–445 (2002).

[49] M. Hindry and J.H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics **201**, Springer-Verlag, New York (2000).

[50] D. Holmes, *Canonical heights on hyperelliptic curves and effective $\mathbb{Q}$-factoriality for arithmetic surfaces*, Preprint (2010). arXiv:math/1004.4503v1 [math.NT]

[51] D. Holmes, *Heights on hyperelliptic curves and a practical algorithm for saturation*, Preprint (2010).

[52] P. Hriljac, *The Néron-Tate Height and Intersection Theory on Arithmetic Surfaces*, PhD thesis, MIT (1983).

[53] P. Hriljac, *Heights and Arakelov's intersection theory*, Amer. J. Math. **107**, 23–38 (1985).

[54] R.W.H.T. Hudson, *Kummer's Quartic Surface*, University Press, Cambridge (1905).

[55] J. Igusa, *Arithmetic variety of moduli for genus two*, Ann. of Math. **72**, 612–649 (1960).

[56] R. Klinzmann, *Normalisierung und Aufblasung arithmetischer Flächen*, Diploma thesis, TU Berlin (2009).

[57] J. Kollár, *Polynomials with integral coefficients, equivalent to a given polynomial*, Electron. Res. Announc. Amer. Math. Soc. **3**, 17–27 (1997) (electronic).

[58] S. Lang, *Introduction to algebraic and abelian functions*, Springer-Verlag, New York (1983).

[59] S. Lang, *Fundamentals of diophantine geometry*, Springer-Verlag, New York (1983).

[60] S. Lang, *Introduction to Arakelov theory*, Springer-Verlag, New York (1988).

[61] M. Laska, *An algorithm for finding a minimal Weierstrass equation for an elliptic curve*, Math. Comp. **38**, 257–260 (1982).

[62] Q. Liu, *Modèles minimaux des courbes de genre deux*, J. reine angew. Math. **453**, 137–164 (1994).

[63] Q. Liu, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*, Trans. Amer. Math. Soc. **348**, 4577–4610 (1996).

[64] Q. Liu, *Courbes stables de genre 2 et leur schéma de modules*, Math. Ann. **295**, 201–222 (1993).

[65] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford University Press, Oxford (2002).

[66] P. Lockhart, *On the discriminant of a hyperelliptic curve*, Trans. Amer. Math. Soc. **342**, 729–752 (1994).

[67] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp., 24, 235–265 (1997). (See also the Magma home page at `http://magma.maths.usyd.edu.au/magma/`.)

[68] Michael B. Monagan, Keith O. Geddes, K. Michael Heal, George Labahn, Stefan M. Vorkoetter, James McCarron and Paul DeMarco, *Maple 10 Programming Guide*, (Maplesoft, Waterloo ON, Canada, 2005) (See also the Maple homepage at `http://www.maplesoft.com`).

[69] H. Matsumura, *Commutative algebra*, W.A. Benjamin, New York (1970).

[70] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Birkhäuser, Boston, 313-334 (1991).

[71] R.L. Miller, *Empirical evidence for the Birch and Swinnerton-Dyer conjecture*, Ph.D. thesis, University of Washington (2010).

[72] J. Milne, *Arithmetic Duality Theorems*, Academic Press, Boston (1986).

[73] J.S. Müller, *Explicit Kummer surface formulas for arbitrary characteristic*, LMS J. Comput. Math. **13**, 47–64 (2010).

[74] `http://www.math.uni-hamburg.de/home/js.mueller`

[75] D. Mumford, *Tata lectures on theta I*, Birkhäuser, Basel-Boston (1983).

[76] Y. Namikawa and K. Ueno, *The complete classification of fibers in pencilos of curves of genus two*, Manuscripta Math. **9**, 143–186 (1973).

[77] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps loceaux et globeaux*, Publ. I.H.E.S. Math. **21**, 361–482 (1964).

[78] A. Néron, *Quasi-fonctions et hauteurs sur les variétes abéliennes*, Ann. Math. **82**, 249–331 (1965).

[79] PARI/GP, version `2.3.4`, Bordeaux (2008)
`PARI/GP` is available from: `http://pari.math.uni-bordeaux.fr`.

[80] F. Pazuki, *Minoration de la hautuer de Néron-Tate sur les surfaces abeliennes*, Preprint (2008). arXiv:math/0812.2854v1 [math.NT]

[81] F. Pazuki, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes: sur la conjecture de Lang et Silverman*, Thèse de doctorat, Université Bordeaux 1 (2008).

[82] B. Poonen and E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. reine angew. Math. **488**, 141–188 (1997).

[83] J. Romero-Valencia and A.G. Zamora, *Explicit constructions for genus 3 Jacobians*, Preprint (2009). arXiv:math/0904.4537v1 [math.AG]

[84] M. Sadek, *Minimal Genus One Curves*, Preprint (2010). arXiv:math/1002.0451v1 [math.NT]

[85] E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann. **310**, 447–471 (1998).

[86] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York (1984).

[87] J.H. Silverman, *Computing heights on elliptic curves*, Math. Comp. **51**, 339–358 (1988).

[88] J.H. Silverman, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55**, 723–743 (1990).

[89] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York (1995).

[90] C. Stahlke, *Algebraic curves over Q with many rational points and minimal automorphism group*, Internat. Math. Res. Notices 1997 **1**, 1–4 (1997).

[91] W.A. Stein et al., *Sage Mathematics Software (Version 4.5.3)*, The Sage Development Team (2010).
`Sage` is available from `http://www.sagemath.org`

[92] M. Stoll, *On the height constant for curves of genus two*, Acta Arith. **90**, 183–201 (1999).

[93] M. Stoll, *Implementing* 2*-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98**, 245–277 (2001).

[94] M. Stoll, *On the height constant for curves of genus two, II*, Acta Arith. **104**, 165–182 (2002).

[95] M. Stoll, *Computing heights on genus two Jacobians III*, unpublished manuscript (2001).

[96] M. Stoll, *j-points-1.1* (2006), available from:
`http://www.mathe2.uni-bayreuth.de/stoll/programs/index.html`.

[97] M. Stoll, *Rational 6-cycles under iteration of quadratic polynomials*, LMS J. Comput. Math **11**, 367–380 (2008).

[98] M. Stoll *On the average number of rational points on curves of genus 2*, Preprint (2009). arXiv:math/0902.4165v1 [math.NT]

[99] M. Stoll, *Models for Kummer varieties of higher genus curves*, in preparation.

[100] A.G.J. Stubbs, *Hyperelliptic curves*, PhD thesis, University of Liverpool (2000).

[101] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, **306** (1965/66).

[102] H. Tschöpe and H. Zimmer, *Computation of the Néron-Tate height on elliptic curves*, Math. Comp **48**, 351–370 (1987).

[103] Y. Uchida, *Canonical local heights and multiplication formulas for the jacobians of curves of genus 2*, Preprint (2009).

[104] K. Yoshitomi, *On height functions on Jacobian surfaces*, Manuscripta Math. **96**, 37–66 (1998).